VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA FINANCÍ

Posouzení ziskovosti těžby kryptoměn za vybraných podmínek

Assessing the Profitability of Cryptocurrency Mining under Specific Conditions

Student: Bc. Michal Ondruš

Vedoucí diplomové práce: doc. Ing. Aleš Kresta, Ph.D.

Ostrava 2018

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra financí

Zadání diplomové práce

Student: **Bc. Michal Ondruš**

Studijní program: N6202 Hospodářská politika a správa

Studijní obor: 6202T010 Finance

Téma: Posouzení ziskovosti těžby kryptoměn za vybraných podmínek
Assessing the Profitability of Cryptocurrency Mining under Specific Conditions

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Úvod
2. Popis kryptoměn a způsobů těžby
3. Teoretická východiska a popis metodiky
4. Posouzení ziskovosti těžby
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

KRÁL, Bohumil a kol. *Manažerské účetnictví*. 3. dopl. a aktualiz. vyd. Praha: Management Press, 2010. ISBN 978-80-7261-217-8.
POPPER, Nathaniel. *Digital Gold: The Untold Story of Bitcoin*. London: Penguin Books, 2015. ISBN 978-0-241-18099-0.
ZMEŠKAL, Z., D. DLUHOŠOVÁ a T. TICHÝ. *Finanční modely: koncepty, metody, aplikace*. 3. přeprac. a rozšíř. vyd. Praha: Ekopress, 2013. ISBN 978-80-86929-91-0.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Aleš Kresta, Ph.D.**

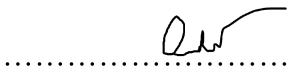
Datum zadání: 24.11.2017
Datum odevzdání: 27.04.2018

Ing. Iveta Ratmanová, Ph.D.
vedoucí katedry

prof. Dr. Ing. Zdeněk Zmeškal
děkan fakulty

„Prohlašuji, že jsem celou diplomovou práci, včetně všech příloh, vypracoval samostatně.“

V Ostravě dne 27. 4. 2018



……

Michal Ondruš

Poděkování

Tímto bych chtěl poděkovat doc. Ing. Aleši Krestovi, Ph.D. za neuvěřitelně vhodné rady a profesionální přístup. Jak řekl Seneca: „ Čas je půjčka, kterou nemůže vrátit ani vděčný dlužník“. Přesto děkuji hlavně za čas, který mi věnoval, ikdyž měl mnoho důležitějších věcí na práci. Více takových lidí . . .

Obsah

1 Úvod

Od počátku lidstva až po dnešní dny se liší názory jednotlivých lidí na rozličné otázky bytí. Mnoho lidí je silně věřících a mnoho zase zatvrdlých ateistů, spousta lidí Vám bude tvrdit, že komunismus je nejlepší a uskutečnitelný projekt společnosti, a spousta lidí vyrukuje s glorifikováním kapitalismu. Neshody s námi byly vždy a vždy budou. Z takových neshod a názorových diferencí však vyvstal také bitcoin, první kryptoměna, jejímž posláním bylo alternovat již zaběhlým metodám tvorby a kontroly peněz ve společnosti. Přes počáteční těžkosti se z bitcoinu stal fenomén, který přilákal velké množství lidí z řad laické veřejnosti, profesionálních investorů a nadšencům cryptoanarchie. Přesto jen malá skupina těchto lidí vidí za bitcoinem onu krásnou liberální ideu nezávislé měny, načež většina lidí vidí jen peníze a možnost rychlého zbohatnutí. Je však ještě možné při takto velkém nárůstu konkurence zbohatnout, zejména pak těžbou bitcoinů ?

Cílem diplomové práce je posoudit ziskovost těžby bitcoinu, jelikož se však jedná o relativně nové téma, tak též seznámení čtenáře s tímto tématem.

Práce je rozdělena do pěti kapitol, přičemž kapitola první je úvodem, jež slouží k seznámení s obsahem a cílem diplomové práce. Závěr je věnován rekapitulaci práce.

Druhá kapitola je zaměřena na charakteristiku bitcoinu. Zpočátku je sepsán vývoj této kryptoměny se zaměřením na nejdůležitější okamžiky v průběhu období let 2009 – 2018. Kapitola pokračuje popsáním ekonomických myšlenek korespondujících s principy bitcoinu a popisem základních charakteristik bitcoinu. Stěžejní část kapitoly je věnována principu těžby bitcoinů. Kapitola je zakončena soupisem možných způsobů těžby, přičemž způsob využíváný v praktické části je podroben detailnějšímu popisu.

Ve třetí kapitole je popsána metodologie, která představuje teoretické východisko pro čtvrtou kapitolu. Text je strukturován tak, že je nejprve popsán princip finančního modelování, načež je demonstrována simulace náhodného vývoje ceny finančního aktiva spolu s definováním základních principů simulace Monte Carlo. Následujicí část kapitoly je věnována investičnímu rozhodování se zaměřením na jednotlivé fáze investičního procesu, kritéria a parametry hodnocení projektů a náklady kapitálu.

Ve čtvrté kapitole jsou nejprve sepsány vstupní data spolu s předpoklady týkající se praktické části. Následuje popis simulace náhodného vývoje ceny bitcoinu a hash rate pro tři

vybrané varianty, je popsán pravděpodobný vývoj těchto veličin v rámci vybraných intervalů spolehlivosti. Ziskovost těžby bitcoinu je posouzena v předposlední části kapitoly. S využitím metody čisté současné hodnoty jsou demonstrovány výsledky jednotlivých variant. Kapitola je ukončena shrnutím dosažených výsledků diplomové práce.

2 Popis kryptoměn a způsobů těžby

Tato kapitola je pro celou práci v podstatě klíčovou. Budou zde popsány nejdůležitější informace vztahující se k bitcoinům a podstatě této práce, tudíž těžby této kryptoměny. Kapitola bude začínat velmi stručnou historií Bitcoinu, neboť to autor považuje za důležité vzhledem k novosti tématu. V podkapitole věnované historii bude práce zaměřena zejména na nejdůležitější okamžiky v průběhu let existence Bitcoinu, neboť podrobnou historii by nebylo možné popsat na několika stranách. Následně bude vysvětlena podstata bitcoinu, kdy bude pozornost zaměřena na důležité aspekty kryptoměn a jejich fungování z hlediska ekonomického a technického. Technickému hledisku bude vyčleněna také třetí podkapitola, kde bude vysvětlen princip těžby bitcoinu. Kapitola bude zakončena informacemi ohledně způsobů těžby, přičemž způsob zvolený k aplikování v praktické části bude podroben bližšímu vysvětlení.

Na začátku je potřeba vysvětlit některé důležité pojmy, které se v práci objevují a jejichž neznalost by mohla vést k nepochopení práce.

ADRESA – Identifikace příjemce platby, reprezentována dlouhým číslem zakodovaným v řetězci alfanumerických znaků určitých vlastností.

ASYMETRICKÁ KRYPTOGRAFIE – Kryptografické metody využívající rozdílnosti šifrovacího a dešifrovacího klíče. Tato skutečnost dává adresátovi zašifrované zprávy možnost nesdílet s odesílatelem zprávy dešifrovací klíč (privátní klíč), ale pouze veřejný klíč. Za pomocí digitálního podpisu, který je vytvořen na základě privátního klíče, lze odeslat určité množství bitcoinů, aniž by daný klíč musel zveřejnit, přičemž ostatní mohou tuto transakci i tak ověřit.

BITCOIN - Nejrozšířenější kryptoměna, která vznikla k roku 2009 a jejíž značka je BTC.

BITCOINOVÁ SÍŤ – Jedná se o decentralizovanou peer-to-peer síť v internetu, v rámci níž dochází ke správě veškerých transakcí mezi všemi uzly sítě.

BLOCK- Nejdůležitější datová struktura protokolu bitcoinu. Ve své podstatě jde o zakodovanou množinu transakcí, které jsou potvrzeny vznikem bloku a jeho validací. Blok, jež má být považován za validní, musí mít vybranou kryptografickou vlastnost, přičemž splnění je velmi náročné na výpočetní výkon.

BLOCKCHAIN – Řetězec validních bloků. Návaznost jednotlivých bloků je zajištěna zahrnutím hashe předchozího bloku do bloku následujícího. Princip blockchainu je popsán dále.

HASH – vyobrazení kvanta dat libovolné délky do množiny dat délky omezené. Například zobrazení textu národní hymny do retězce o 64 znacích.

HASHOVACÍ RYCHLOST – hashovací rychlost udává velikost výpočetního výkonu bitcoinové sítě nebo jednotlivých uzlů v síti. Základní jednotkou této rychlosti je h/s, neboli počet hashů vypočtených za jednu sekundu. Vzhledem k velkému výpočetnímu výkonu dnešních těžících zařízení jsou využívány odvozené jednotky jako 1 kh/s (1000 h/s) Mh/s (1 000 000 h/s) atd.. Dnešní výkon (1. 2. 2018) je počítán v řádu desítek EH/s (1 000 000 000 000 000 000 h/s).

KRYPTOMĚNA – Kryptoměnou se rozumí digitální měna využívající techniky šifrování a hashování k její tvorbě a ověřování všech transakcí.

PRIVÁTNÍ KLÍČ –Jeden z párů klíčů příslušící každé bitcoinové adrese. Tento klíč umožňuje odeslání bitcoinů z konkrétní adresy, proto by měl zůstat tajný. Slouží také k dešifrování zprávy určené majiteli adresy spojené s tímto privátním klíčem. Za použití techniky „HD Wallets“ může jeden privátní klíč náležet více adresám majitele.

PENĚŽENKA –Software určený ke správě privátních klíčů náležících k bitcoinovým adresám uživatele,provádění plateb nebo zaznamenávání transakční historie.

VEŘEJNÝ KLÍČ –Druhý z páru klíčů náležících bitcoinové adrese, který může kdokoliv využít k zašifrování informace pro majitele privátního klíče nebo k verifikaci jeho digitálního podpisu. V rámci bitcoinové sítě je veřejný klíč využit k výpočtu adresy uživatele.

TĚŽBA – Těžbou dochází k ověření provedených transakcí a následnému vytvoření bloku, který je dále napojen do blockchainu. Těžbou také vznikají nové bitcoiny, jež jsou v podstatě odměnou těžaři za poskytnutý výpočetní výkon sloužící k potvrzení transakcí a vytvoření bloku.

TRANSAKCE – datová struktura obsahující dvě množiny (vstupy, výstupy), přičemž vstup odkazuje na výstup v již existující transakci. Zjednodušeně je to pouze informace ohledně převodu bitcoinů z adresy na jinou adresu.

2.1 Stručná historie Bitcoinu

V první podkapitole druhé kapitoly bude stručně popsána historie Bitcoinu od roku 2009 až po současnost. Protože nelze zmínit každou významnou událost doprovázející vývoj Bitcoinu, budou prezentovány pouze události, které se staly významnými milníky Bitcoinu na krkolomné cestě k dnešní popularitě.

2.1.1 Prvopočátky Bitcoinu

Jedny z prvních myšlenek na vytvoření kryptoměn pocházely z mozků lidí prohlašující sebe za tzv. cypherpunkery. Cypherpunker je kdokoliv, obhajující využití kryptografie a technologií zlepšujících soukromí, jako prostředek k dosažení sociální a politické změny. První zmínky aktivního hnutí cypherpunkerů pocházejí z 80 let, kdy byly vydány práce kryptografa Davida Chauma na téma anonymní digitální měna v knize s poměrně liberálním názvem Security without Identification: Transaction Systems to Make Big Brother Obsolete (David Chaum, 1985). Od daného roku se postupně rozšiřovala základna lidí považujících se za cypherpunkery a rostl též počet důležitých projektů, které byly těmito lidmi vytvořeny.

Myšlenky a nápady na vytvoření digitální měny byly denním chlebem mnohých cypherpunkerů. Postupně docházelo ke zdokonalování procesů stojících za dnešními kryptoměnami, přičemž byla v průběhu těchto let vytvořena (prací Davida Chauma) digitální měna, s podstatu vystihujícím názvem, ecash. Protože však tato měna nevyužívala princip blockchainu, typický pro Bitcoin, brzo společnost zajišťující její kontrolu zanikla. Z toho důvodu bylo potřeba vytvořit měnu s využitím do té doby ještě neznámého principu. A právě vytvoření blockchainu, tzv. účetní knihy obsahující záznamy o všech transakcích, doprovázelo vytvoření kryptoměny Bitcoin.

O vytvoření Bitcoinu se v roce 2009 zasloužil vývojář s pseudonymem Satoshi Nakamoto, který tak učinil na základě průvodního článku publikovaného v roce předchozím. Nakamoto tvrdil, že na vývoji Bitcoinu pracoval už od roku 2007, což znamená, že vysoce sofistikovanou technologii podpírající bitcoin vytvořil za úžasné dva roky. Protože se ovšem neví, kdo za tímto projektem ve skutečnosti stojí, je možné, že se jedná o skupinu odborníků na kryptografii, informatiku a ekonomii, neboť přijít s tak elegantním řešením a technologií by samotnému člověku trvalo s největší pravděpodobností déle.

Je důležité poukázat na skutečnost, že Satoshi Nakamoto přenechal po rozšíření této kryptoměny doménu bitcoin.org fanouškovi projektu a pozdějšímu primárnímu vývojáři kódu

bitcoinu Gavinovi Andersonovi, načež se nadobro odmlčel. Je tedy patrné, že za vytvořením projektu nestála vidina rychlého a značného zbohatnutí, ale naopak vytvoření konkurenčního finančního systému, jež by vzal moc velkých bank a privilegovaných elit a vrátil ji všem jednotlivcům. Toto tvrzení podporuje i fakt, že většina prvních nadšenců a uživatelů bitcoinů se rodila z řad liberálů, a celkově lidí hledajících alternativu k zaběhlému systému.

Satoshi Nakamoto byl také prvním, kdo vytěžil blok bitcoinů v roce 2009. Tomuto bloku se dnes přezdívá tzv. blok genesis a má následující podobu:

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Protože však Nakamoto usiloval o mnohem vyšší cíle, bylo nutné „přilákat" k této měně co nejvíce uživatelů, a zajistit aby tito uživatelé mezi sebou prováděli transakce. Z toho důvodu provedl Nakamoto historicky první transakci, kdy poslal první bitcoiny vývojáři a nadšenci jménem Hal Finney, jehož jméno je ve světě bitcoinu jedním z nejznámějších.

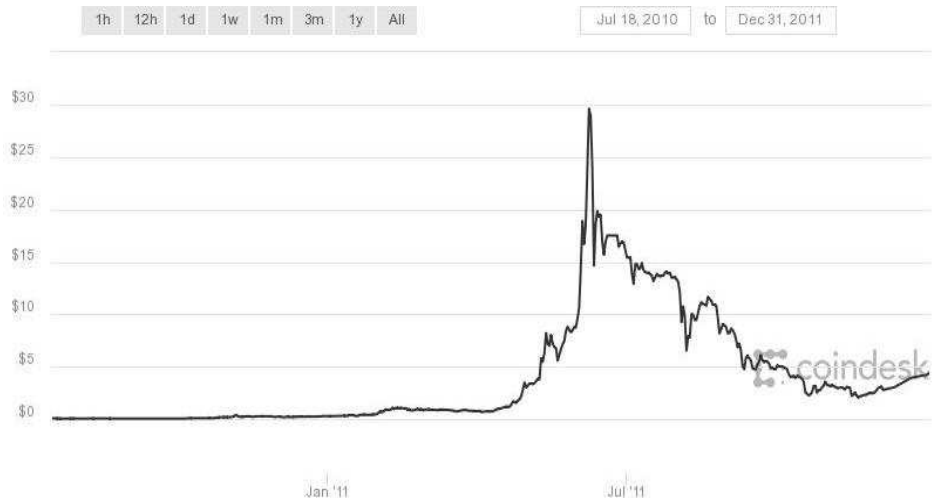
Transakce se povedla a nyní bylo na pořadu dne, aby se našel někdo, kdo bude ochotný za tuto měnu zaplatit, neboť právě tohle je podstata úspěchu. Čím více lidí je ochotno si danou měnu koupit a obchodovat s ní, tím úspěšnější se projekt stává. Doba, po kterou za měnu nikdo nebyl ochotný zaplatit více, než náklady na těžbu, dosáhla jednoho a půl roku. Poté se na fóru bitcointalk.org zjevila nabídka ve znění: Zaplatím 10 000 bitcoinů za pár pizz…Tuto nabídku učinil floridský programátor se jménem Laszlo Hanyecz. A opravdu se našel člověk, který byl ochoten přijmout 10 000 BTC za dvě pizzy v hodnotě 25 dolarů. Z dnešního pohledu se může člověk chytat za hlavu, neboť hodnota bitcoinů razantně narostla, nicméně právě tento okamžik s největší pravděpodobností vedl k počátečnímu růstu hodnoty bitcoinu. Navíc právě tato transakce potvrdila podstatu bitcoinu jako nástroje možného k placení za reálné věci.

Rok 2010 byl tedy pro bitcoin zlomovým rokem z výše popsaných důvodů. Došlo také k vytvoření první burzy s bitcoiny Mt.Gox, první transakci mezi telefony, první veřejně známé půjčce, objevila se první bitcoinová opce a v České republice vznikl první těžební pool založený Markem Palatinusem.

V roce 2011 dosáhl bitcoin parity s dolarem, což znamená, že byl obchodován za 1 dolar, viz graf 2-1. V průběhu roku postupně narůstal, zejména díky nabídek k směně různorodých věcí za bitcoiny, přičemž bitcoin začaly přijímat i některé nové e-shopy. Největším milníkem tohoto roku byla jednoznačně možnost posílat bitcoiny serveru WikiLeaks, jemuž byl zablokován jakýkoliv příjem peněžních prostředků z důvodu zveřejňování citlivých informací

ohledně americké špionážní síti nebo mučení vězňů v Iráku. Možností tento server podporovat i přes všelijaké zákazy pomohl Bitcoinu získat opravdovou popularitu, čímž pochopitelně rostla i jeho cena. Netrvalo to ovšem dlouho a bitcoin zažil největší propad ve své historii. V době kdy tržní kapitalizace bitcoinu dosahovala výše 200 milionů dolarů, klesla hodnota bitcoinu během čtyř dní z 31.91 dolarů na 10 dolarů. Tomuto krachu se přezdívá Velká bublina roku 2011, a že byla opravdu velká, ilustruje fakt, že se bitcoin na hodnotu 31,91 dolarů dostal až koncem února roku 2013. Docházelo také k prvním krádežím, které pokračovaly i v dalších letech, přičemž největší z nich se odehrála v návaznosti na krádež hesel z burzy Mt.Gox, která měla za následek příkazy na prodej stovek tisíc bitcoinů. Kvůli této umělé nabídce klesla hodnota v červnu roku 2013 z 18 dolarů na téměř nulovou hodnotu.

Graf 2-1: Vývoj ceny bitcoinu v období 2009 - 2011



Zdroj: http://www.coindesk.com

Přesto se mnoho lidí stojících za tímto projektem nevzdalo a začaly pořádat první konference. První z nich se odehrála v New Yorku, načež následovala též konference v Praze, jejímiž účastníky byly lidé z evropských koutů světa. Díky této snaze o propagaci Bitcoinu začala jeho cena opět pomalu růst.

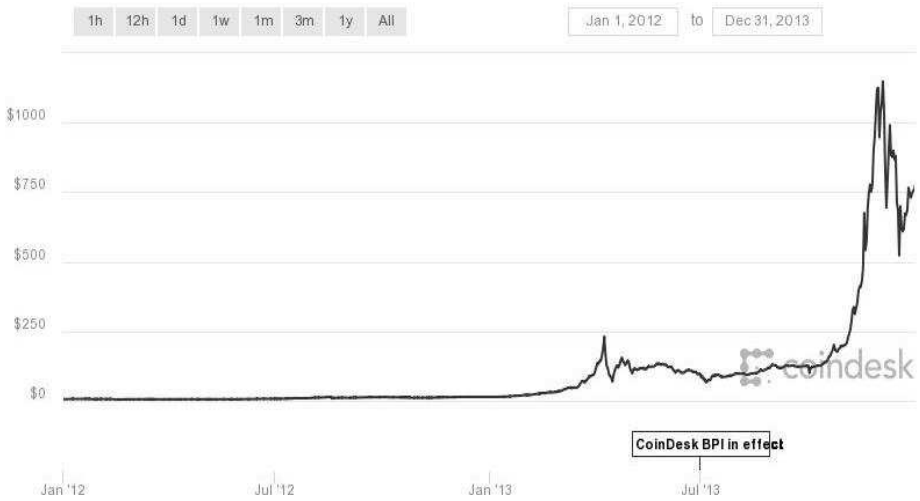
2.1.2 **Období 2012 – 2013**

V letech 2012 a 2013 se zvyšoval počet lidí využívajících bitcoin a také počet společností usilujících o jeho začlenění do možných způsobů plateb v těchto společnostech. Jako nejvýznamnější společnost lze zmínit publikační platformu WorldPress, jež umožnila uživatelům odkup placených služeb za bitcoiny. Důvodem začleňování bitcoinů k platebním metodám v ostatních společnostech (restaurace, e-shopy) bylo zavedení okamžitého převodu

bitcoinů na dolary za minimální poplatek společností BitPay.com. Společnosti tedy mohly přijímat bitcoin, aniž by tuto měnu ve skutečnosti museli krátkodobě držet v rámci svých aktiv. V říjnu 2012 zareagovala taktéž Evropská centrální banka zprávou[1], ve které se ECB snažila Bitcoin nekritizovat, ba dokonce ho představuje v dobrém světle, a pouze poukázala na možnost zhoršení reputací centrálních bank evropských zemí v důsledku nástupu kryptoměn.

Důležitým odvětvím, jež zvyšovalo popularitu bitcoinu, byl také hazard. Příčinou je následující skutečnost. Klasické hazardní služby z důvodu zdanění a regulací navyšují své zisky pomocí tzv. zvýhodnění podniku, tedy průměrné procento zisku kasina, které v některých případech dosahuje až 50 % (ruleta má zvýhodnění 5,26%). Díky Bitcoinu začaly vznikat hry, jako například SatoshiDice, kde zvýhodnění kasina nedosahuje ani zdaleka zvýhodnění například rulety. Není tedy divu, že spoustu lidí přitahuje hra SatoshiDice, v rámci které je zvýhodnění 1.9 %, zejména kvůli nedanění zisků a nulové regulace. Je ovšem jasné, že i tato hra bude muset své zvýhodnění snížit, přičemž je možno dostat se až na nulu, neboť konkurence bude tlačit toto zvýhodnění neustále dolů. Spojení Bitcoinu a hazardu je tedy vynikajícím příkladem dokonalé konkurence, o které se mnoho ekonomů vyslovuje ve svých knihách.

Graf 2-2: Vývoj ceny bitcoinu v období 2012 - 2013



Zdroj: http://www.coindesk.com

Od roku 2012 do konce roku 2013 dosáhla tržní kapitalizace bitcoinu hodnoty miliardy až desíti miliard dolarů, aby hned na přelomu let 2013 a 2014 dosáhla tržní kapitalizace maxima na více než 14 miliardách dolarů.Co se týče ceny této měny, bitcoin dosáhl hodnoty sta dolarů v dubnu roku 2013, načež koncem tohoto měsíce vzrostla hodnota až na vysokých 266 dolarů.

[1] Odkaz: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Za rok tedy přidal obrovských 2 000 %. Následně však bublina splaskla a bitcoin se dostal na 150 dolarů, což ovšem nebyl zvláště vysoký propad. Cena začala opět růst s tím, jak začaly bitcoin přijímat další a další organizace. Stroukal (2018) ve své knize uvádí například internetového prodejce Overstock, Univerzitu v Nikósii nebo basketbalový tým Sacramento Kings. Docházelo též k určitým výzvám, kdy se reportérka časopisu Forbes snažila vyžít v rámci placení kryptoměnami. Ačkoli uznala, že daná cesta přežívání není snadná, svým příspěvkem vzkázala také to, že pomocí bitcoinu se přežít dá. Spolu s novomanžely Austinem a Beccy Craigovými, kteří se nechali dokumentaristy po dobu 100 dní natáčet, jak jezdí po světě a platí pouze bitcoiny, efektní cestou ukázali, že bitcoiny lze považovat za peníze.

O Bitcoinu psal skoro každý. Vznikaly první knihy, webové magazíny, časopisy a audio pořady. Téměř všechna periodika chtěla informovat ohledně nárůstu popularity Bitcoinu. Na světlo světa ovšem přicházely také falešné zprávy o údajných regulacích a zákazech obchodování s Bitcoinem, jež údajně vydávaly například centrální banky. S každou takovou zprávou rostla panika mezi novými uživateli, neboť ne každý měně zcela rozuměl. Negativní a lživé zprávy byly skoro vždy následně vyvráceny a panika zmizela.

V pozadí toho všeho stále rostl význam tzv. Silk Road. Jednalo se o ilegální server, na kterém bylo nabízeno na deset tisíc různých produktů (převážně drogy), a jehož využívání stálo a padalo na možnosti obchodu s bitcoiny. Celkové tržby serveru za dva roky přesáhly miliardu dolarů, přičemž se provedlo přes 1,2 milionů transakcí. Jednalo se tedy o velmi důležitý článek, jež napomáhal zvyšování zájmu o tuto kryptoměnu, ale také dokázal pořádně zahýbat s její cenou. Přestože příběh Silk Road nekončí idylicky, zakladatel Ross Ulbricht byl zatčen a server zanikl, napomohl k popularizaci Bitcoinu a jeho rozšíření. Poslední informaci ještě umocňuje fakt, že zadržené bitcoiny Rosse Ulbrichta byly vydraženy v aukci, což dodalo Bitcoinu známku legality. Paradoxem však nakonec byla snaha mnohých o znovu založení podobně fungujícího serveru, načež začaly vznikat mnohem sofistikovanější verze. Snaha o regulaci Bitcoinu se tak ukázala jako situaci ještě zhoršující.

2.1.3 **Období 2014-2015**

Konec roku 2013 byl ve znamení růstu ceny na rekordní hodnotu 1 163 dolarů za jeden bitcoin. Následně bitcoin začal klesat, dokud se jeho cena neustálila na hodnotě mezi 800 – 900 dolary. To bylo v lednu 2014. S počátkem února toho roku ovšem přišla jedna z nejvýznamnějších událostí v historii kryptoměn. Burza Mt.Gox, jeden z nejdůležitějších

článků popularity bitcoinu, přestala vyplácet peníze a zbankrotovala[2]. Na základě této události klesla cena Bitcoinu až k 340 dolarům.

Figure 2-3: Vývoj ceny bitcoinu v období 2014 - 2015

Zdroj: http://www.coindesk.com

Rok 2014 byl poznamenán také dobrými zprávami. Britský úřad pro výběr daní a cel prohlásil bitcoiny za soukromé aktivum, jak uvádí Stroukal (2018), což znamenalo, že není povinností z této měny platit DPH. Na druhou stranu se postavila Evropská unie, která skrze European Banking Authority vydala dokument, ve kterém vyjasňuje svůj postoj ke kryptoměnám a navrhuje statut povinných osob všem burzám kryptoměn. Ty by poté musely hlásit objemy peněz protékající skrze tyto burzy, což by zlepšilo dohled nad praním špinavých peněz nebo transakcemi teroristickým organizacím. Celkově se ale kryptoměnám v Evropě dařilo, o čemž vypovídá i nákup bitcoinů ministrem financí Velké Británie, čímž poukázal na svůj pozitivní vztah k Bitcoinu. Problémy se začaly rýsovat na druhé straně zeměkoule, v New Yorku, kde se vyskytly první snahy o návrh skutečné regulace kryptoměn.

Také na české scéně se Bitcoinu velmi dařilo. Zaprvé byla spuštěna první hardwarová peněženka nazvaná Trezor, jejíž pomocí mohl uživatel výrazně zlepšit ochranu Bitcoinů v jeho portfoliu. Zadruhé byl uměleckou skupinou Ztohoven otevřen institut cryptoanarchie Paralelní Polis, v rámci kterého jsou pořádány odborné přednášky na téma kryptoměn, ale nejen to. Existuje zde bitcoinový bankomat a kavárna, ve které je dovoleno platit pouze bitcoiny.

[2] Podrobnější informace o krachu Mt.Gox lze najít v knize Bitcoin a jiné kryptopeníze budoucnosti, jež je uvedena v seznamu literatury na konci práce.

Ačkoli došlo v roce 2014 k vyššímu propadu ceny, neznamenalo to propad zájmu o tuto kryptoměnu. Právě naopak. Například přední výrobce softwaru Microsoft se koncem tohoto, výrazně negativního roku z hlediska ceny, rozhodl přijímat bitcoiny

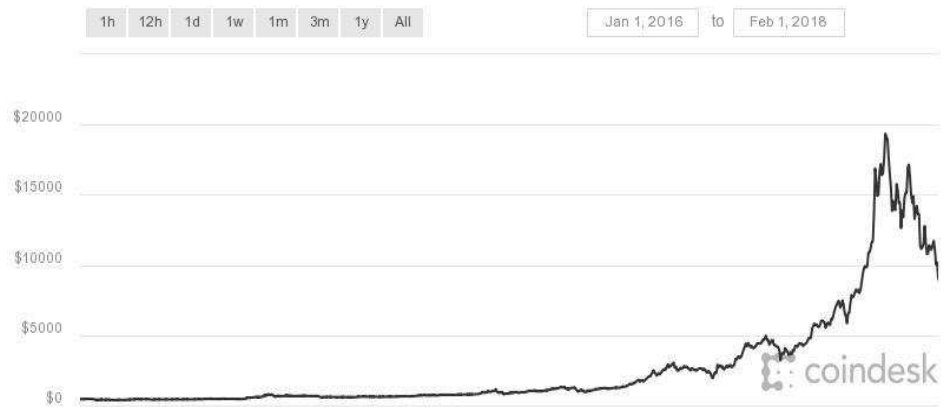
V roce 2015 se situace stabilizovala a nastal klid. Přibyly důležité firmy přijímající bitcoin, mezi nimiž lze jmenovat například Dell, T-Mobile v Polsku, Twitch.tv, Movietickets v USA a čerpací stanice Lukoil v Pobaltí spolu s dalšími tisíci malými podniky po celém světě. Vznikaly nové pokusy o využití kryptoměn v erotickém a porno průmyslu. V září téhož roku spustila Čína rozsáhlé kapitálové kontroly, jež vyústily v úprk investorů spolu s mnoha miliardami dolarů. Čína se snažila pomoci ekonomice kontrolou přeshraničního toku financí, což následně vyústilo v růst ceny bitcoinu. Další dobrou zprávou bylo rozhodnutí Evropského soudního dvoru ve věci bitcoinu a DPH. Soud rozhodl o tom, že se DPH nevztahuje na Bitcoiny, čímž rozhodl vleklý spor ve Švédsku, které se snažilo považovat bitcoin za určitý druh zboží. V návaznosti na všechny tyto a jiné důvody se cena bitcoinu, po nárůstu na 500 dolarů, začala konsolidovat v pásmu 300-400 dolarů

2.1.4 **Rok 2016 – současnost**

První z těchto dvou let, tedy rok 2016, byl ve znamení poklidnějšího růstu, a to nejen cenového, ale i růstu využívání bitcoinu. V březnu 2016 označila japonská vláda bitcoin za aktivum podobné reálným penězům, přičemž následující rok ho plně zlegalizovala. Nejvýznamnější norská online banka začala nabízet bitcoinové účty a ruská vláda začala mluvit o spolupráci s kryptoměnami.

Přibývalo opět obchodů začínajících přijímat bitcoin jako oficiální platidlo, mezi nimi se objevily firmy jako Steam, Bidorbuy nebo Alza, největší český e-shop. Celkově za rok 2016 došlo k ztrojnásobení obchodů přijímajících bitcoin a využívajících jeho služeb. Ve Venezuele se měna začala využívat jako alternativa k národní měně, zejména z důvodu hyperinflace zabraňující spoření v domací měně. Díky Bitcoinu se některým obyvatelům země podařilo ochránit proti masivnímu znehodnocování a byli schopni koupi letenky pomocí níž by odcestovali ze země. To vše a ještě více se začalo projevovat v ceně bitcoinu, jež začala narůstat a do konce roku 2016 dosáhla téměř dvojnásobné hodnoty.

Graf 2-4: Vývoj ceny bitcoinu v období 2016 - 2018



Zdroj: http://www.coindesk.com

Rokem 2017 pak začalo něco nepředstavitelného. Cena Bitcoinu se z hodnoty 1 000 dolarů vyhoupla na hodnotu blízkou 20 000 dolarů, k čemuž došlo ke konci roku 2017. Mnoho lidí považovalo danou událost za klasickou bublinu na trhu finančních aktiv, avšak Bitcoin už v minulost zažil podobných procentních nárůstů cen několik, nikdy ovšem tak dlouhodobých. V pozadí rozhodovalo mnoho faktorů, jako například růst popularity měny, začleňování dané měny do běžných ekonomických činností a rozhodně i chtíč zbohatnout. Nárůst ceny se ale neobešel bez problémů postihující vše populární a úspěšné.

Pochopitelně začalo přibývat krádeží, z nichž největší se odehrála v srpnu 2016. Tehdy jedna z největších burz Bitfinex přišla o 120 tisíc bitcoinů. Na rozdíl od pádu Mt.Gox se nicméně nejednalo o velmi vážný problém, neboť burza slíbila ztráty uhradit a navíc se nejednalo o jedinou entitu, jejíž pomocí lidé bitcoin mohli používat, jako v případě Mt.Gox. Vznik bitcoinových směnáren a bankomatů značně umožnil nakládání s bitcoiny a burzy se staly spíše posvátným místem spekulantů a obchodníku s velkými objemy.

Větší problém nastal z hlediska počtu transakcí v bitcoinové síti. Původní nastavení měny zajišťovalo fixní počet transakcí za jednotku času, což nevyhovovalo razantnímu nárůstu počtu uživatelů bitcoinu a síť přestala stíhat. Více lidí z komunity bylo pro zachování stávajícího systému, zejména z důvodu zpětné kompatibility a silnější decentralizace. Protiargumentem menší skupiny byla větší propustnost sítě a levnější transakce. Členové komunity přišli s kompromisem, který zaručil větší propustnost spolu s možným systémovým vylepšením v budoucnu, kdy bude řešení více propracované. Proti něčemu takovému se ovšem

postavila velká komunita čínských těžařů z okolí společnosti Bitmain, neboť navrhovaná změna těmto těžařům znemožnila způsob těžby, který do této doby používali, a který zvyšoval efektivnost těžby o 20 %. Protože se daného způsobu těžby nechtěli vzdát, založili novou kryptoměnu s názvem Bitcoin Cash. Ta po třech měsících dosáhla hodnoty půlky bitcoinu, aby ovšem následně spadla na šestinovou cenu.

Jedná se o názorný úkaz internetové svobody a lidské vynalézavosti z nespokojenosti. Když se někomu něco nelíbí, má možnost vytvořit nástroj dle vlastního uvážení, přičemž úspěch stojí a padá s originálností a precizností vytvořené alternativy. Bitcoin je jedním z průkopníků kryptoměn a momentálně nejoblíbenější a nejvíce hodnotnou kryptoměnu. Po vzoru Bitcoin Cash a jiných, začíná ovšem vznikat stále více a více nových kryptoměn, mající různé cíle a softwarové pozadí. Jejich vývoj v budoucnu bude záviset na mnoha faktorech, stejně jako budoucnost Bitcoinu. Tato budoucnost je determinována postojem vlád, centrálních bank, komunitou kryptoanarchistů, veškerou veřejností, ale zejména flexibilitou v řešení příchozích problémů, kterých může v budoucnu přibývat.

2.2 Podstata

Podstatou v této kapitole je míněn popis nejdůležitějších charakteristik kryptoměn, jmenovitě bitcoinu. Nejprve bude Bitcoin velmi stručně popsán z hlediska ekonomické teorie, která je blízká podstatě bitcoinu. Následně budou objasněny nejdůležitější atributy a pilíře, které podpírají fungování této kryptoměny. Podkapitola bude zakončena náhledem do budoucnosti a představením možných problémů, jenž mohou v budoucnu bitcoin ohrozit a způsobit pokles jeho hodnoty.

2.2.1 Ekonomická teorie

Ačkoli dnes většina lidí vnímá kryptoměny pouze jako prostředek k investici, tedy určitou obdobu komodit, jejich idea a podstata je založena na myšlenkách, které velmi korelují s myšlenkami ekonomů neoliberalismu či rakouské školy, jak uvádí Stroukal (2018). Důležitými rysy tohoto směru je návrat k idejím ekonomického liberalismu a myšlenkám řízení trhu na principu laissez-faire. Ekonomové zastávající názory rakouské školy prosazují myšlenky směřující ke snižování účasti státu na jeho ekonomice a zasazují se o snižování byrokracie, daní nebo státních výdajů. Mezi ekonomy rakouské školy patřili velikáni ekonomie jako Carl Menger, Friedrich von Wieser, Eugen vin Bohm-Bawerk, Ludwig von Mises a Friedrich Hayek. Velkým přínosem rakouské školy bylo dílo Carla Mengera z roku 1871, kde

bylo prvně využito analýzy na základě mezních veličin, což významně obohatilo a změnilo obor ekonomie jako takový.

Ekonomové této školy, jmenovitě Hayek a Mises, velmi kritizovali socialismus a vyvrátili možnost racionální kalkulace za tohoto režimu, čímž vlastně tvrdili, že centrální plánovač nemá praktickou možnost kvalitně plánovat, neboť není schopen získat veškeré potřebné informace, jež udává trh. Už zde je tedy vidět, že se ekonomie rakouské školy staví do opozice vůči pokusům monopolizovat důležité funkce ekonomiky do rukou vybrané instituce. Daná myšlenka se objevuje též v teorii hospodářského cyklu formulované těmito dvěma významnými ekonomy, jak demonstruje Stroukal (2018). V ní Mises a později také Hayek zdůrazňují negativní vliv centrálního bankovnictví, přičemž uvádí výhody svobodné soutěže i v rámci peněz. Je tedy možné vidět určité paralely mezi fungováním bitcoinu a myšlením ekonomů rakouské školy, neboť právě bitcoin se snaží o tzv. denacionalizaci peněz, což ve své podstatě znamená odstřihnutí kontroly nad tvorbou peněz od centrálních bank. Mnoho ekonomů rakouské školy vidí východisko ve vrácení a udržení zlata ve finančním systému jako základ hodnoty peněz. Místo zlata by však časem mohl zastat právě bitcoin pro své vlastnosti, jež jsou zlatu velmi podobné, zejména konečné množství, které se dá vytěžit. Na rozdíl od zlata lze ovšem bitcoin dělit v podstatě donekonečna, což odráží argument mnohých odpůrců ohledně nedostatečné zásoby komodity. Problémem je dnes pouze určitá skepse vůči Bitcoinu, neboť mnoho lidí stále ještě takzvaně Bitcoinu nepřišlo na chuť a nevnímají Bitcoin jako něco, co zlato může nahradit. Je tedy otázkou času jakým směrem se bitcoin v budoucnu posune.

Poslední myšlenka je věnována teorii hospodářského cyklu. Dle teorie hospodářského cyklu je narušení cenového systému příčinou vzniku mnoha krizí v minulých stoletích. Znehodnocením peněz centrální bankou narušuje ceny a informace v nich obsažené. To může vést ke špatným rozhodnutím, která vedou k nadměrnému zadlužování a výběrům neefektivních projektů firmami. Na základě následného procitnutí, kdy například původně levné úvěry zdražují, může dojít z důvodu velké propojenosti ekonomiky, k výrazným problémům, jež známe například z poslední krize z roku 2008. Protože je bitcoinů omezené množství a nelze je jednoduše tisknout podle potřeb, odpadá problém umělé expanze peněžní zásoby, jenž způsobuje dle ekonomů rakouské školy hospodářské cykly. Jedná se samozřejmě pouze o teorii, kterou je velmi obtížné empiricky ověřit, nicméně pokud by se daná teorie někdy ukázala jako pravdivá, jednalo by se o velmi důležitý pokrok na poli ekonomie. (Stroukal, 2018)

2.2.2 **Charakteristika Bitcoinu**

Bitcoin je dnes synonymem pro virtuální měnu, přesto přesnějším označením by byl název bitcoinová siť nebo protokol, neboťjde o síť vzájemně komunikujících počítačů v režimu peer-to-peer (rovný s rovným). Způsob peer-to-peer umožňuje decentralizaci, hlavní pilíř kryptoměn, narozdíl od režimu připojování klient server, kde existuje centrální autorita shromažďující data. V režimu peer-to-peer sdílí každá jednotka soubory se všemi ostatními, což aplikováno na Bitcoin znamená, že se v podstatě jedná o všemi uživateli v síti sdílenou informaci o tom, že daný uživatel vlastní určité množství bitcoinů.

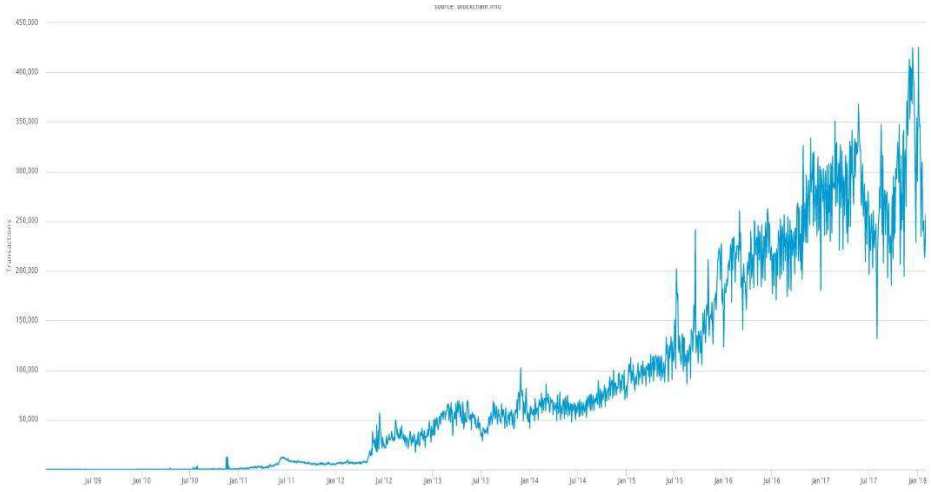
V klasickém pojetí vznikají peníze jednak samotným tiskem bankovek centrální bankou, a jednak v rámci procesu úvěrování obchodními bankami, které vytváří bezhotovostní formu peněz. Se zvyšujícím se objemem peněz v ekonomice klesá jejich kupní síla, což známe pod pojmem inflace. Protože peníze nejsou vázány například na zlato, je jejich počet téměř neomezen, stejně tak jako možné znehodnocení, které prakticky okrádá lidi o úspory. V tomto centralizovaném systému tedy může životy milionů lidí ovlivnit poměrně úzká skupiny lidí v čele centrálních a obchodních bank. Zavedením Bitcoinu by mohly být tyto problémy odstraněny.

Pokud by šlo Bitcoin k něčemu přirovnat, tak ke zlatu. Podobně jako u zlata je bitcoinů konečné množství a k jejich získání je potřeba těžit. Satoshi Nakamoto navrhl systém tak, že do něj implementoval konečné možné množství vytěžených bitcoinů v počtu 21 milionů. Zdali je to málo nebo hodně není podstatné a to z následujícího důvodu. Mnoho lidí argumentovalo v neprospěch zlatého standardu z důvodu konečného množství zlata, jež by nemělo stačit na tvorbu dostatečného množství peněz v budoucnu. Protože je bitcoin digitální, není konečný počet žádnou překážkou, neboť jednotlivé bitcoiny lze dělit teoreticky donekonečna a bez obtíží, které by s tímto procesem nastaly u zlata. Nyní je základní jednotkou 1 BTC, který je možno dělit až na 8 desetinných míst. Dalšími jednotkami jsou tyto následující:

- *1cBTC = 0.01 BTC (centibitcoin),*
- *1mBTC = 0.001 BTC (milibitcoin),*
- *1μBTC = 0.000001 BTC (mikrobitcoin),*
- *1 Satoshi = 0.00000001 BTC – nejnižší jednotka.*

Bitcoin, jako každá jiná měna, by měl plnit základní funkce peněz. První funkcí, kterou autor práce považuje za nejdůležitější, je funkce *směny a měřítka cen*. Je podstatné aby bylo možné využít konkrétní měnu k nákupu statků a služeb, což ovšem z počátku nebylo možné. Jak bylo zmíněno v kapitole věnující se historii, daná funkce se začala postupně rozvíjet v okamžiku, kdy bylo nabídnuto větší množství bitcoinu za nákup pizzy. Od této chvíle až dodnes se počet transakcí razantně zvýšil, jak je partné z grafu 2-5, což v konečném důsledku pozitivně ovlivňovalo také růst ceny. Lidé a společnosti začali přijímat bitcoin jako možný prostředek k nákupu produktů, a ačkoli se jedná v celosvětovém měřítku o malé procento subjektů přijímajících bitcoin, důležité je, že tento počet narůstá. Navíc se jedná o věc relativně novou a mnoha lidmi zatím nepochopenou. S tím, jak bude příbývat diskusí a článků o této měně, stále více lidí bude přicházet kryptoměnám na chuť a celkové množství subjektů směnujících bitcoin za své služby či produkty naroste ještě více. Zdali bude bitcoin v budoucnu všeobecně přijímaným platidlem nelze stoprocentně říct, jeho dočasný vývoj ovšem signifikuje, že by tomu tak mohlo v budoucnu býti.

Graf 2-5: Počet transakcí za den pro období 2009 - 2018

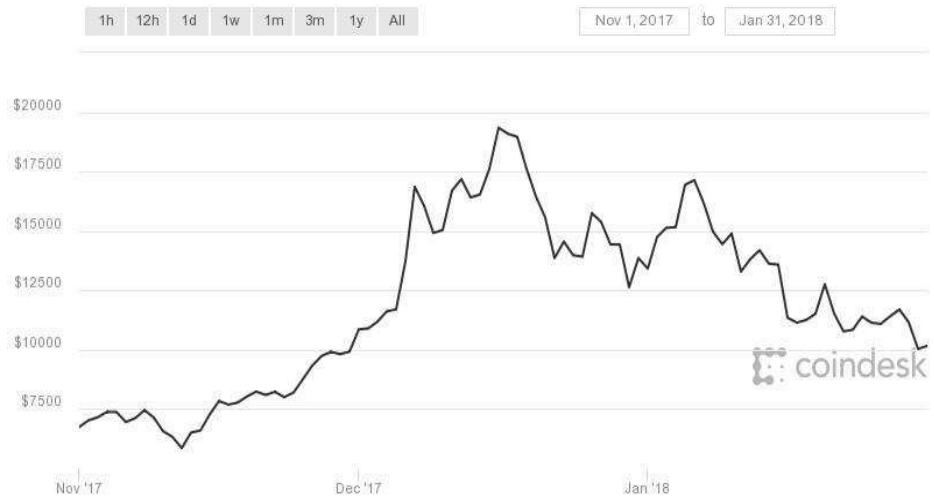


Zdroj: www.blockchain.info

Zdali je možné považovat bitcoin za uchovatele hodnoty, záleží zejména na přítomném optimismu ohledně budoucího vývoje. Bitcoin samozřejmě hodnotu má a tato hodnota výrazně narostla, nicméně vysoká volatilita této měny vyobrazená v grafu 2-6 a nejistota ohledně budoucího vývoje, můžou tuto hodnotu značně snížit, v nejhorším případě až na samotné dno. Navíc neexistuje žádná centrální autorita, která by se zavázala k udržení hodnoty dané měny, jako například Centrální banka. Na základě těchto skutečnostní je bitcoin snažší považovat více za nástroj ke spekulaci, než uchovatel hodnoty. Aby bylo možné považovat bitcoin za uchovatel

hodnoty, měla by se cena ustálit a volatilita snížit, což je ovšem v blízké budoucnosti cíl poměrně nemožný, vzhledem k tomu, že většina lidí v Bitcoinu vidí pouze nástroj ke spekulaci, nikoli jeho pravou podstatu.

Graf 2-6: Volatilita ceny bitcoinu Listopad 2017 - Únor 2018



Zdroj: www.coindesk.com

Jestliže však neexistuje žádná centrální instituce zaručující se za danou měnu, tedy její falšování a znehodnocování, jak bitcoin vzniká a funguje z tohoto hlediska? Roli centrální autority zde zastává právě decentralizovaný systém celé sítě. Veškeré transakce, vznik bitcoinů a jejich potvrzení jsou ověřovány soustavně všemi uzly v síti při činnosti nazývané těžba.

2.3 Princip těžby

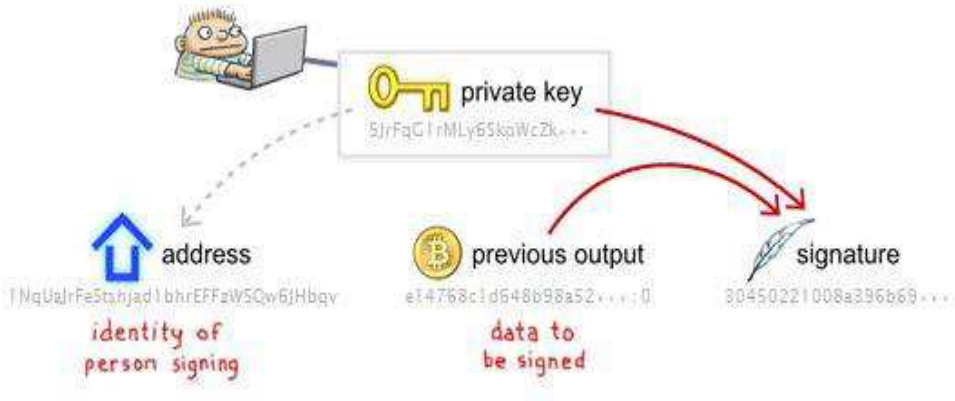
Aby mohl kdokoliv využívat bitcoin a platit jím, je potřeba aby pro něj byla vygenerována unikátní bitcoinová adresa (řetězec dlouhý 34 písmen a čísel) a korespondující privátní klíč k této adrese. V případě provedení transakce z určité adresy je nutné tuto transakci potvrdit užitím tohoto privátního klíče. Pomocí sérií komplexních matematických úloh[3] je privátní klíč navázán na danou adresu, přičemž je prakticky nemožné tento klíč získat z adresy pomocí zpětného řešení matematických funkcí, čímž je zajištěna důvěryhodnost tohoto systému.

S privátním klíčem může kdokoliv poslat peníze jinému uživateli, aniž by však tento klíč bylo nutné zveřejnit. K tomu je využíván tzv. digitální podpis, viz obr 2-1. Uživatel

[3]Odkaz: https://www.coindesk.com/math-behind-bitcoin/

jednoduše vloží svůj privátní klíč spolu s detaily transakce do softwaru, jež běží na jeho počítači. Aniž by došlo k poslání těchto informací do sítě, speciální software tyto informace zakóduje skrze komplikované matematické rovnice do kódu, nazývaného digitální podpis. Tento digitální podpis je poté odeslán spolu s transakcí, podobně jako by kdokoliv podepisoval například šek.

Obr. 2-1: Vytváření digitálního podpisu



Zdroj: www.preshing.com

Počítače, které dostanou tento digitální podpis, nejsou schopny zpětnými výpočty zjistit privátní klíč, avšak tyto počítače mohou adresu a digitální podpis podrobit řadě matematických funkcí a potvrdit, že daný digitální podpis byl vytvořen pomocí privátního klíče korespondujícího s danou veřejnou adresou. Důležité je znovu podotknout, že matematika v pozadí těchto procesů je vysoce sofistikovaná, jak na straně vytvoření podpisu, tak při jeho verifikaci. Verifikace sama o sobě je velmi důležitou komponentou v rámci fungování bitcoinu, neboť neexistuje centrální autorita, jež by danou věc dělala. Pomocí složitých výpočtů je poté transakce potvrzena, jak je znázorněno v obr. 2-2.

Obr. 2-2: Princip potvrzení transakce

Zdroj: www.preshing.com

Tímto však celá transakce nekončí. Počítače v síti poté musí prostudovat veškeré transakce z minulosti týkající se daných bitcoinů, jež mají být zaslány, aby bylo zjištěno, že konkrétní uživatel opravdu disponuje bitcoiny, které se snaží odeslat. A právě v rámci verifikace na scénu nastupují těžaři. Aby bylo možné vysvětlit, co vlastně tito těžaři dělají, bude jako první vysvětlena kryptografická hashovací funkce.

Kryptografické hašovací funkce se využívají pro ověřování autenticity a integrity zpráv nebo pro zajištění bezpečnosti hesel. V procesu těžby bitcoinu a ověřování transakcí je hashovací funkce jeden z klíčových pojmů. Velmi zjednodušeně hashovací funkcí rozumíme proces, který z množství vstupních znaků jakékoliv délky (vstupní řetězec) vytváří výstup s fixním počtem znaků (digest, hash). Ať je vstupní řetězec tedy slovem, větou nebo celou knihou, výstup bude vždy stejně dlouhý. Klíčovou vlastností je také následující fakt. Pokud dojde ke změně velmi malé části vstupu, výstup bude naprosto odlišný od předchozího. Tato skutečnost je velmi důležitá pro celkovou náročnost těžby, jak bude popsáno ještě dále. V bitcoinových protokolech jsou hashovací funkce součástí block-hashing algoritmu, který se využívá k zápisu nových transakcí v rámci bitcoinové sítě do blockchainu pomocí samotné těžby. Vstupem pro tyto funkce jsou ještě nepotvrzené transakce spolu s dalšími vstupy zahrnující odkazy na předchozí transakce, viz obrázek 2-3.

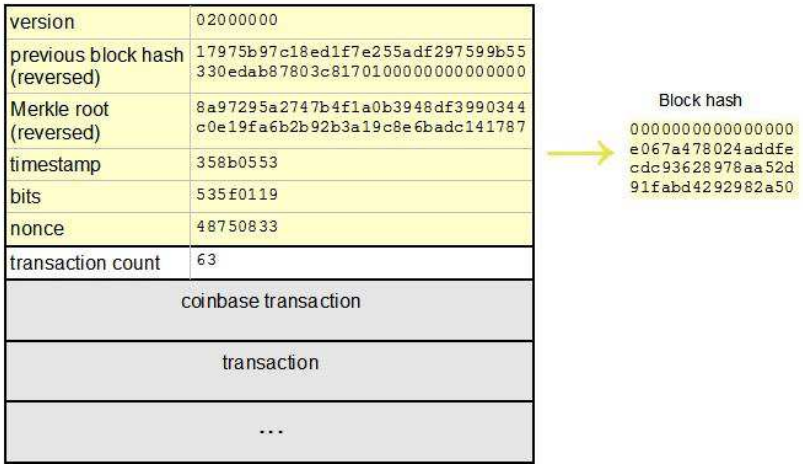
Satoshi si všiml toho, že by bylo velmi problematické, kdyby každý počítač v síti zaznamenal transakci v čase, kdy se k němu dostala. Tím by docházelo k tomu, že by určitý počítač obdržel konkrétní transakci dřív, než by dorazila k počítačům dalším. Bylo nutné vytvořit takový systém, aby vznikl pouze jeden definitivní záznam o konkrétní transakci. Satoshi Nakamoto došel k zajímavému řešení tohoto problému. Toto řešení je zajímavé v tom, že jím Satoshi Nakamoto vytvořil určitý závod v hledání řešení, v rámci kterého mohou soutěžit všechny počítače v síti.

Počítače v síti postupně ukládají jednotlivé transakce, tak jak byly poslány po síti, do dlouhých seznamů, známé jako bloky. Poté co počítač uloží transakce do bloku, začne tento blok podrobovat speciálním matematickým rovnicím, též hash funkcím, přičemž výsledkem je 64znakový řetězec. Počítače, které se tohoto procesu účastní, hledají takový blok, který může být vložen do hash-funkce známé jako SHA 256 a který vygeneruje 64znakový řetězec se specifickým počtem nul na začátku. Například pokud je vyhledáván řetězec s pěti nulami na počátku, může být vítězný řetězec následující:

000008e77563ddd1914847k369ui147w444ss9vbng1234hjki23564mvvcd7852

Pod odstavcem uvedený obrázek zobrazuje strukturu specifického bloku. Žlutou část tvoří hlavička bloku, pod kterou jsou uspořádány jednotlivé transakce v bloku. Tzv. coinbase transakce je transakce pomocí níž vznikají nové bitcoiny v síti, což bude vysvětleno dále. Hlavička bloku se skládá postupně z verze protokolu a haše předchozího bloku, jež zaručuje návaznost všech bloků v blockchainu. Merkle root je haš všech transakcí v bloku a je zodpovědný za nenávratnost transakce po jejím provedení a zařazením do bloku. Timestamp symbolizuje časový údaj ohledně daného bloku, jenž je následován řádkem bits, což je hodnota určující obtížnost těžby. Posledně nonce je náhodné číslo přidávané ke každému bloku v rámci zkoušení nalezení toho pravého. Zjednodušeně řečeno těžař vkládá informace uvedené v žluté části obrázku 2-3 do hashovací funkce, přičemž k dané struktuře přidává náhodné číslo, které slouží k odlišení generovaného řetězce za účelem nalezení bloku.

Obr. 2-3: Sturktura bloku



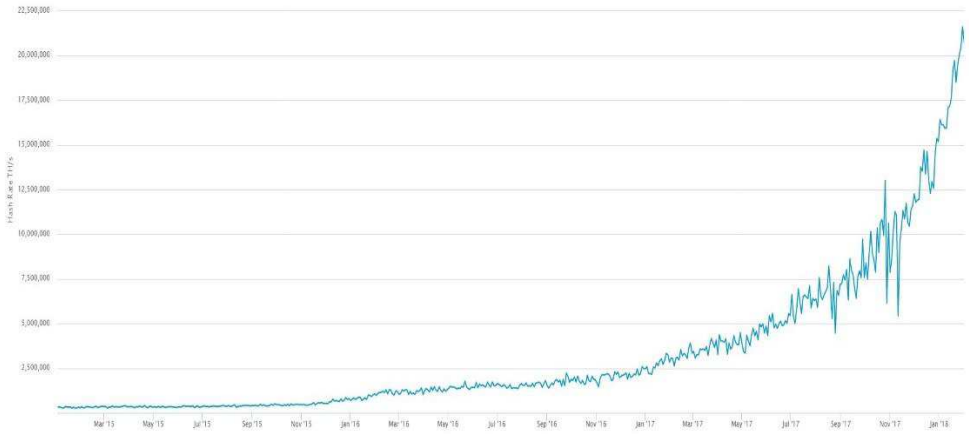
Zdroj: www.righto.com

Jelikož je SHA 256, obdobně jako ostatní hash-funkce, odolná vůči obrácenému postupu výpočtu, je prakticky nemožné říci, který blok povede k číslu o pěti nulách na počátku. Technika s nulami na začátku je velmi elegantním řešením narůstajícího výkonu celé sítě, neboť pomocí navýšení nul se obtížnost zvýší v poměru k síle početního výkonu, aby byl čas mezi nalezením bloku přibližně konstantní v čase.

Protože z podstaty SHA 256 a dalších hash-funkcí vyplývá, že z konkrétního vstupu bude vygenerován vždy stejný výstup, pokud by každý počítač v síti zadal do bloku stejné transakce, dostal by každý počítač také stejný řetězec v rámci výstupu. V návaznosti na daný problém, je k odlišení bloků využíván princip přidávání náhodných čísel na konec bloku *(nonce)* každým počítačem v očekávání nalezení správného řetězce, přičemž například malá změna

tohoto čísla z 20 na 22 může způsobit změnu řetězce z řetězce o dvou nulách na deset. Jestliže dané číslo nevede k nalezení řetězce o specifickém počtu nul na počátku, počítače budou dále zkoušet nová čísla spolu s přidáváním dalších transakcí do bloku, dokud někdo daný blok nezíská, tedy číslo se správným počtem nul na začátku. Protože však náhodné přidávání čísel je víceméně hrou náhody, získání bloku bude s největší pravděpodobností v režii těžaře nebo seskupení těžařů mající největší výpočetní výkon. Výpočetní výkon (hash rate) je zde počítán pomocí jednotky H/s (haš za sekundu), tedy kolik možností k nalezení bloku přístroj vyzkouší za jednu sekundu. Dnešní nejvýkonější přístroje typu ASIC mají výpočetní výkon roven několika TH/s, terrahash za sekundu, což odpovídá 1 000 000 000 000 H/s. Celkový hash rate sítě je potom součtem všech těžících zařízení těžících konekrétní měnu. Vývoj celkového hashrate je vyobrazen na v grafu 2-7.

Graf 2-7: Vývoj hashrate v období 2015 - 2018



Zdroj: www.blockchain.info

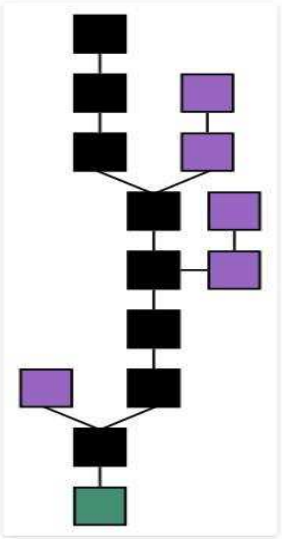
Dnešní výpočetní výkon sítě se pohybuje v hodnotách EH/s (exahash), což je 1 000 000 TH/s. Od data 25. 1. 2016, kdy byla tato hodnota poprvé překonána, stoupl k 1. 2. 2018 celkový výpočetní výkon na hodnotu vyšší než 20 EH/s. V rámci výpočtu očekávaného počtu vytěžených bitcoinů je dané číslo podstatné, neboť podíl těžařova výkonu na celkovém výkonu sítě určuje přibližné množství bitcoinů, jež vytěží.

Jakmile někdo z těžařů najde vítězný blok, pošle se tento blok skrze celou síť, aby mohli ostatní těžaři daný blok verifikovat a potvrdit, že tento blok opravdu generuje skrze hašovací funkci číslo s požadovaným počtem nul na počátku. Poté je tento blok přidán k předchozím blokům do *blockchainu*, aby byla zaručena návaznost jednotlivých transakcí v blocích. Jestliže

není v daném bloku zařazena některá transakce z období generování tohoto bloku, bude tato transakce přidána do hledání bloku následujícího.

Blockchain je v podstatě účetní kniha obsahující veškeré transakce, které na síti od prvopočátku proběhly. Obrázek zobrazuje 2-4 podstatu blockchainu.

Obr. 2-4: Struktura blockchainu



Zdroj: www.en.wikipedia.org

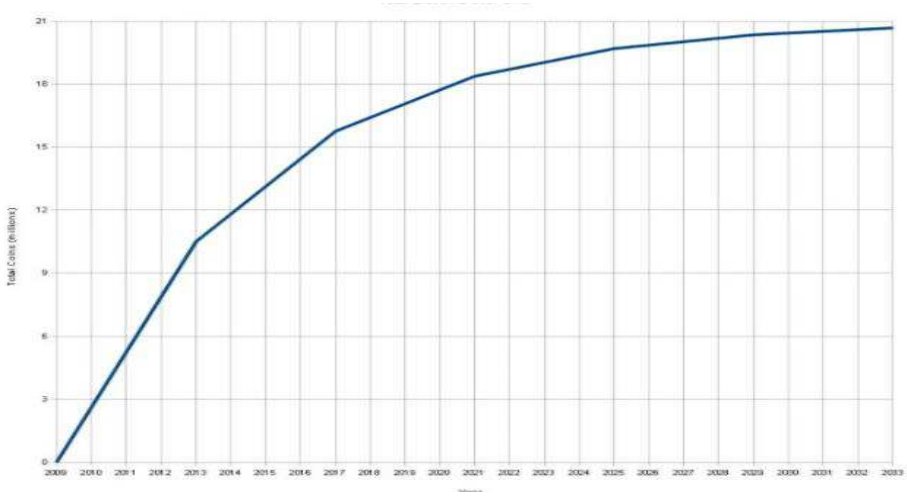
Zelený blok symbolizuje historicky první vytěžený blok v síti, jenž je též nazýván jako Genesis. Černé bloky zobrazují bloky, které byly potvrzeny většinou v síti a přídány do validního blockchainu. Protože různé skupiny těžařů pracují na jiných blocích, může se stát, že různé skupiny budou chtít zanést do blockchainu jiné záznamy transakcí a dojde k rozvětvení blockchainu, které reprezentují fialové bloky v obrázku. To by znamenalo, že jednotlivé skupiny těžařů vedou rozdílné účetní knihy. Aby se tomuto problému zabránilo, jako platný blockchain je brán ten, který má vytěžený větší počet bloků. Jak je vidět v obrázku 2-4, druhý černý blok navazuje na transakce prvního, čímž je řetězec dlouhý tři bloky (počítaje Genesis blok). Naproti tomu rozvětvěný fialový blok zahrnující odlišné transakce je v podstatě jeden jediný. Jako správný blockchain je tedy vybrán černý a problém dvojité útraty je zažehnán, vyjma 51% útoku, kdy by někdo s nadpolovičním výkonem v rámci sítě mohl určovat validitu blockchainu sám.

Na závěr je potřeba zmínit následující. Aby měl někdo vůbec chtíč těžit a potvrzovat transakce, musel vzniknout takový systém, aby těžaři také získali něco navíc, určité množství bitcoinů. Proto při každém nalezení bloku získává těžař, který daný blok najde, odměnu ve výši

50 bitcoinů (dnes tj.1. 2. 2018 už 12.5 – odměna se snižuje každých 2016 bloků). Tato odměna vzniká tak, že v rámci přidávání transakcí k nalezení vítězného bloku, je do tohoto bloku také přidána transakce zaručující určitý počet bitcoinů pro výherce. Proto s nalezením bloku je verifikována též tato transakce a vzniká nový počet bitcoinů v síti. Tento počet je ovšem daný a nikdo si nemůže nárokovat více než konkrétní počet bitcoinů, neboť v případě, že by si chtěl přidat například dvojnásobek, došlo by při následné verifikaci k zamítnutí bloku. Těžař také získává určitý počet bitcoinů z poplatků na provedení transakcí zahrnutých v bloku.

Jak již bylo zmíněno, maximální počet bitcoinů je 21 milionů, což vzhledem k exponenciálnímu snižování odměny a parametrům systému znamená, že tyto bitcoiny budou vytěženy v roce 2140, avšak obrovská většina bude vytěžena už k roku 2030, viz graf 2-8.

Graf 2-8: Předpokládaný nárůst množství bitcoinu v oběhu



Zdroj: www. commons.wikimedia.org

Aby množství bitcoinů rostlo tempem navrženým Satoshim Nakamotou, tedy v návaznosti na myšlenku, aby veškeré mince nebyly vytěženy v průběhu velmi krátkého období, využívá bitcoin, mimo snižování odměny, princip proměnlivé obtížnosti k nalezení bloku. Těžba bitcoinu je navržena tak, aby byl jeden blok vytěžen v průměru jednou za 10 minut. To znamená, že s rostoucím výpočetním výkonem roste také obtížnost nalezení ve stejném poměru.

Pro lepší pochopení bude uveden jednoduchý příklad, který by měl pomoci čtenáři k pochopení přizpůsobování obtížnosti celkovému výpočetnímu výkonu. Dejme tomu, že velké množství lidí háže kostkou. Každý miliontý hod se podaří všem najednou hodit šestku, čímž najdou pomyslný blok. Jestliže víme, že blok má být nalezen každých 600 sekund, je velice

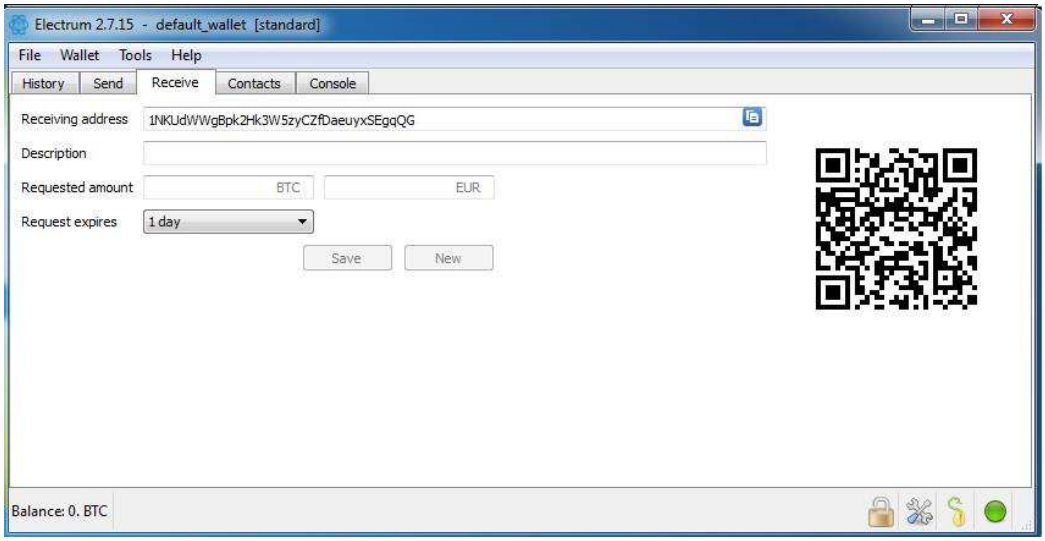
lehké zjistit, kolik hodů kostkou je potřeba udělat za sekundu aby byl blok nalezen. Je to cca. 1 667 hodů za sekundu (hash rate). A cílem změny obtížnosti je nastavit počet nutných hodů k nalezení bloku na takové číslo, aby při změně rychlosti hodů za sekundu, zůstala doba nalezení bloku na 600 sekundách. To lze udělat například zvýšením počtu házejících lidí. Tím je zaručeno, že k vytěžení bitcoinů nedojde v krátké době.

2.3.1 Využití vytěžených bitcoinů

Přidat se a provádět transakce, těžit nebo nakupovat bitcoiny je dnes záležitostí velmi snadnou a časově nenáročnou. Nejdříve je potřeba založit si svou peněženku, aby mohly být bitcoiny někde ukládány. Obdobně jako při užívání klasické měny může uživatel důvěřovat sobě nebo jiným.

Jedním z možných řešení pořízení peněžky, je stáhnutí softwaru z oficiálního klienta z webu bitcoin.org. Tento klient v sobě obsahuje celý blockchain a jeho velikost dosahuje 150 GB dat, přičemž bude neustále narůstat. Nejedná se tedy o vhodnou variantu pro lidi s měnším úložným prostorem v počítači. Úspornějším řešením je například program Electrum, který lze jednoduše nainstalovat do počítače jako datový soubor a následně pomocí něj vygenerovat pěněženku. Soubor je poté potřeba uložit a zálohovat způsobem podobným jako v případě uschování čehokoliv důležité a cenného v životě. Jakmile je vytvořená peněženka, je také vytvořena její adresa, viz obrázek 2-5.

Obr. 2-5: Bitcoinová peněženka



Zdroj: www. blog.coingate.com

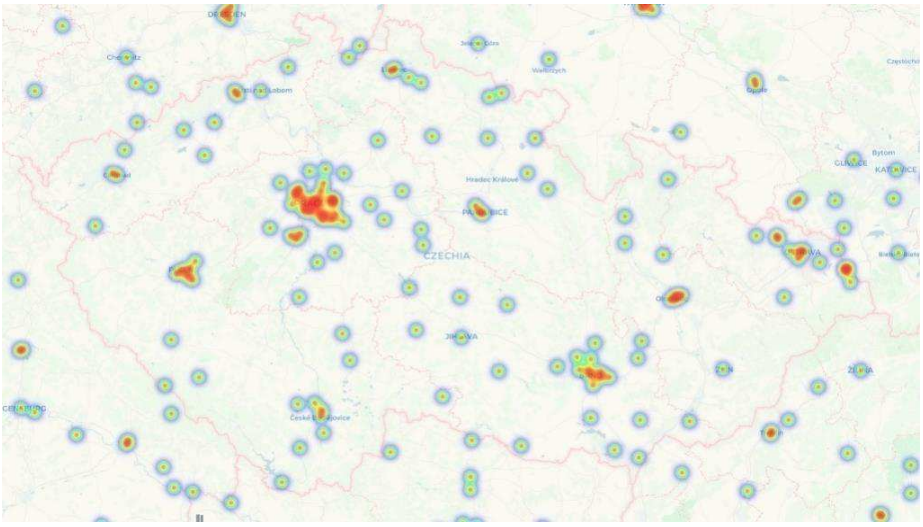
V záložce receive a send jsou možnost přijetí a odeslání bitcoinů, přičemž v případě přijetí stačí adresu zaslat komukoliv, kdo by vám chtěl bitcoiny poslat. V případě disponováním bitcoinů je možné je odesílat na předem domluvenou adresu. Při odesílání je důležité vědět, že toto posílání není úplně zadarmo. K transakci je zahrnut poplatek ve výši např. jedné tisíciny bitcoinu, avšak je možné tento poplatek navýšit a upřednostnit vaší transakci před jinými, čímž dojde k jejímu rychlejšímu vyřízení.

Další možností je vytvoření peněženky online například na webu coinbase.com nebo blockchain.info. Nicméně zde musí uživatel důvěřovat třetí straně a počítat s rizikem možného vykradení, což už se mnohokrát v historii měny stalo. Existují též mobilní aplikace pro chytré telefony.

Protože je práce věnována těžbě, nebudou zde popsány možnosti koupě bitcoinu na burzách a směnárnách. Místo toho bude práce věnována prodeji bitcoinu a jeho využití v případě získání určitého množství těžbou.

Jakmile subjekt vytěží určité množství bitcoinů, má v zásadě tři možnosti, jak s ním nakládat. Zaprvé může bitcoin prodat na specializované burze, mezi něž patří například bitstamp.net nebo kraken.com. Druhou možností je nákup zboží nebo služeb v obchodech, které bitcoin přijímají, jako například Alza.cz. Na níže uvedeném obrázku 2-6 jsou vyznačeny místa v ČR, kde je bitcoin přijíman jako standardní měna. Další možností je bitcoin využít ke spekulaci na budoucí nárůst ceny a následnému prodeji.

Obr. 2-6: Místa v České republice přijímající bitcoin



Zdroj: www.coinmap.org

2.3.2 **Budoucnost**

Dle Stroukala (2018) je první hrozbou, kterou je potřeba zmínit, a která by mohla v budoucnu ohrozit fungování bitcoinu, potažmo narušit principy na kterých stojí, regulace. Veškeré kryptoměny vznikly s ideou vytvoření alternativního, a tedy konkurenčního platidla, jež by konkurovalo státům (centrálním bankám), které drží monopol na tvorbu peněžní zásoby. To se ovšem vládám jednotlivým státům pochopitelně nezamlouvá, natož pak řešení problémů s výběrem daní a s kontrolou peněžních toků. To by samozřejmě nebyl problém, pokud by bitcoin tak zásadně nevzrostl v oblibě mnohých lidí. Od konce roku 2013, kdy počet uživatelů bitcoinu činil něco kolem dvou milionů,vzrostl počet uživatelů této kryptoměny na desítky milionů ke konci roku 2017. A proto se budeme čím dál tím více setkávat se snahami implementovat Bitcoin do legislativy s cílem změnit jeho vlastnosti k obrazu vlády. To ovšem na druhou stranu není tak úplně snadné.

Stroukal (2018) uvádí příběh amerického regulátora, který zjistil, že statut bitcoinu jako měny je v rozporu s platnou legislativou. Proto se pokusil sepsat a odeslat žádost o ukončení činnosti, načež se ukázalo, že nemá, komu by danou žádost adresoval. Zprávu tedy poslal na neziskovou organizaci, jež měla slovo Bitcoin v názvu, avšak zpráva zůstala bez odezvy. Bitcoin s sebou totiž nese skutečnou decentralizaci a jeho regulace je obdobně obtížná, jako byla například regulace internetu. Rozdíl je pouze v motivaci Bitcoinu stát se globální měnou, což podkopává jakoukoliv činnost vlády, na rozdíl od internetu. Proto je motivace regulovat Bitcoin mnohem vyšší.

A vlády už se v tomto směru angažovat začaly, jak tvrdí Stroukal (2018). Příkladem lze uvést prohlášení Newyorského finančního kontrolora Bena Lawskyho, který důvodem k regulaci nazývá zejména ochranu spotřebitele, odstranění ilegálních aktivit a ochranu národní bezpečnosti. Také demokratický senátor Chuck Schumer nazval Bitcoin jako prostředek k praní špinavých peněz. Nositel Nobelovy ceny za ekonomii Paul Krugman zase nazval Bitcoin jako plýtvání elektřiny, což ovšem můžeme chápat, pokud je vizí tohohle ekonoma finanční systém, kde kontrolu nad peněžním systémem drží centrální banka, která tento systém nastavuje dle vlastních potřeb nebo potřeb jiných. Jednoduše bude přibývat argumentů nazývajících bitcoin měnou podporující zločiny, jež se pomocí této měny financují. Avšak s přihlédnutím k faktu, že se dneska hotovost využívá k daňovým únikům, praní špinavých peněz a financování terorismu, zůstávají tyto argumenty invalidní.

Ke krokům, jež byly doposavad učiněny, lze zmínit například návrh v Německu, které připravilo kapitálovou daň z držení bitcoinů. Také ve Finsku podléhá výnos z prodeje či těžby kryptoměn kapitálové dani. V České Republice je situace značně odlišná, neboť zatím došlo jen k formulování doporučení, v rámci něhož si mají subjekty na tyto měny dávat pozor, a k prohlášení, jež nařizuje oznamovat transakce přesahující 15 tisíc eur (Stroukal, 2018).

Jak uvádí Stroukal (2018), nejprogresivnější regulace proběhla v Číně, kde Čínská centrální banka zakázala v prosinci roku 2013 všem finančním institucím provádět obchody s bitcoiny. Dané nařízení snížilo cenu bitcoinu, avšak vágní povaha této regulace nezastavila velké čínské burzy v provádění obchodů s bitcoinem. Burza s názvem BTC China a jiné nepřestaly provádět obchody s kryptoměnami, načež objem těchto obchodů začal ještě narůstat. Naproti tomu se Evropská unie staví ke kryptoměnám z opačného konce. Evropský soudní dvůr ve věci platby DPH z bitcounů publikoval 22. října své stanovisko, kde píše[4], že je na bitcoin dle směrnic evropského práva třeba pohlížet jako na měnu, jež je oproštěna od daně z přidané hodnoty. Tím fakticky legitimizoval bitcoin jako měnu.

Regulaci se ovšem bitcoin s nějvětší pravděpodobností nevyhne. Jestliže se má bitcoin stát všeobecně přijímaným platidlem, bude potřeba vytvořit transparentní systém, ve kterém dojde k identifikaci všech uživatelů, čímž se z velké části podaří předejít nelegální činnosti. Přemýšlí se například nad institucionalizovanými peněženkami na způsob bankovních účetů, které budou nést informaci o uživatelích. Protože je bitcoin věcí novou a věčně omílanou, lidé budou přicházet s dalšími možnostmi na lepší transparenci měny a implementaci do stávajícího systému. Jestli se bitcoin stane obdobou současných peněz a lidé podpoří nápad ohledně identifikace uživatelů a placení daní, namísto opačné možnosti, je hudbou blízké budoucnosti.

Bitcoin pro mnoho lidí znamená zásadní revoluci ve světovém finančním systému. Lidé rozličných politických přesvědčení vnímají bitcoin z různých hledisek změny, které nabízí. Pro někoho bitcoin otevírá bránu k omezení vlád nebo k tvorbě konkurence dnešnímu bankovnímu systému. Revoluci může také znamenat v rámci globálního obchodu, kdy snižuje rizika postihující klasické měny, jakým je například riziko devalvace. Velkým pokrokem je také vynález blockchainu, který s sebou nese další využití například pro tvorbu nových sociálních sítí nebo systémů vlastnických práv k finančním, ale i jiným aktivům. Vznikají nové služby, jež usnadňují platby pomocí bitcoinů a zefektivňují tak samotný finanční systém. Je mnoho

[4]Odkaz na stanovisko Evrospkého soudního dvoru:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=604646

dobrých věcí, které s sebou Bitcoin, kryptoměny obecně, přináší. Je ale nadmíru důležité, aby lidé tyto pozitivní stránky vnímali a nesoustředili se pouze na možnost rychlého zbohatnutí. Je sice pravda, že postupem času začíná bitcoin využívat stále více lidí, otázkou je však, zdali se nejedná jen o momentální horečku, která časem nebo s klesající cenou odezní a lidé se vrátí k jediné, do té doby známé klasické měně vydávané centrální bankou.

To jestli bitcoin v budoucnu neupadne v zapomění, jako například Myspace, které zažilo velký růst, ale o to bolestnější pád, záleží na mnohých faktorech, například na regulaci. Zásadní pro jeho přežití je ovšem víra lidí v bticoin a ochota ho využívat jako alternativní platidlo. Přijetí této moderní koncepce měny založené na nových technologiích je pro mnoho lidí prakticky nemožné, zejména pro ty, kteří jsou navyklí starým pořádkům a pro které je už například bezhotovostní forma peněz v podstatě magií. Proto záleží hlavně na lidech nadšených pro danou koncepci.

2.4 Bitcoin mining

Podkapitola o principu těžby je stěžejní částí této práce, neboť dále bude analyzována právě ziskovost samotné těžby. Začátek podkapitoly bude věnován popisu vstupů, jež jsou nepostradatelné pro samotné těžení, načež bude pokračovat představením minulých i nynějších způsobů těžby. Následně bude vylíčen dle autorova názoru nejlepší způsob těžby za konkrétních podmínek, který bude též detailněji představen z důvodu pozdějšího využití v práci. Kapitola bude zakončena popisem principu a průběhu těžby z hlediska procesů odehrávajících se na pozadí dolování bitcoinů.

2.4.1 Těžba bitcoinů

Nyní bude popsán krok za krokem proces těžby v poolu od nákupu těžícího přístroje až po inkasování odměn. Podkapitola bude zakončena představením způsobů těžby a detailnějším popisem vybraného způsobu.

Aby mohl kdokoliv začít těžit bitcoin v dnešní době, je potřeba aby ze všeho nejdříve investoval určitou sumu peněz do nákupu těžícího zařízení, které bude provádět jednotlivé výpočty generující bitcoiny. Existuje mnoho způsobů jakými kryptoměny těžit, nicméně v rámci bitcoinové sítě je dnes využíván pouze hardware specializovaný na výpočet jediné úlohy.Tento hardware využívá ASIC chipy, tedy čipy s integrovaným obvodem, které jsou určeny pro výpočet konkrétní kryptografické funkce náležející k bitcoinu. Existuje tedy určité podnikatelské riziko, kdy nebude možné prodat tento hardware v případě pádu bitcoinu na nulu.

K zařízení využívající ASIC je potřeba dokoupit napájecí zdroj, jež tvoří přibližně desetinu ceny. Jakmile je správně nainstalován hardware, je na řadě instalace těžícího softwaru. Výběr softwaru je odvozen od způsobu těžby a od výběru konkrétního poolu. Například Slushpool, český těžební pool, podporuje těžící software s názvem cgminer a BFGminer. Následujícím krokem je registrace v rámci vybraného poolu a nastavení ASIC zařízení, tedy připojení k serveru konkrétního poolu. Těžící zařízení musí být nasměrováno na jeden ze stratum serverů zobrazených na obr. 2-7.

Obr. 2-7: Servery pro těžbu bitcoinů - Slush pool

Umístění serverů	Adresa
USA, východní pobřeží	stratum+tcp://us-east.stratum.slushpool.com:3333
Evropa	stratum+tcp://eu.stratum.slushpool.com:3333
Čína, pevnina	stratum+tcp://cn.stratum.slushpool.com:3333 stratum+tcp://cn.stratum.slushpool.com:443
Singapore, South Asia	stratum+tcp://sg.stratum.slushpool.com:3333
Japan, Pacific	stratum+tcp://jp.stratum.slushpool.com:3333

Zdroj: www.slushpool.com

Poté stačí zadat přihlašovací údaje potřebné pro konkrétní zařízení, viz obr. 2-8. Jedná se o velice zjednodušené vysvětlení, jež je uváděno na webových stránkách slush poolu[5]. Je potřeba podotknout, že každý těžební pool má jinak nastavené připojení k serverům a navíc se veškerá nastavení těžby liší z hlediska využití konktrétního těžícího zařízení a software.

Obr. 2-8: Nastavení identifikace těžícího zařízení - Slush pool

```
URL: stratum+tcp://stratum.slushpool.com:3333
userID: userName.jménozařízení
heslo: cokoliv
```

Zdroj: www.slushpool.com

Před samotnou těžbou je ještě nutné pořídit si bitcoinovou peněženku, kde budou zasílány jednotlivé výplaty bitcoinů. Jedna z nejpopulárnějších peněženek je program

[5] Odkaz: https://slushpool.com/help/get-started/mining_beginners

Electrum, jež je možné stáhnout a nainstalovat na počítači. Následně vám bude vygenerována peněženka, přičemž se jedná o datový soubor, který je důležité co možná nejlépe chránit před útoky hackerů. Vytvořením peněženky se vytvořila i veřejná adresa, která bude využita jako výplatní adresa, viz obrázek 2-5.

2.4.2 **Náklady na těžbu**

Mimo počáteční náklady na nákup těžících zařízení, vznikají další náklady v průběhu těžby samotné. Jedná se zejména o náklady na spotřebovanou elektřinu, jejichž výše závisí na příkonu těžícího přístroje a době, po které tento přístroj provádí těžbu. Ziskovost těžby tedy z velké části závisí na ceně elektřiny v regionu, ve kterém těžař těží. Pro zajímavost je v tabulce 2-1 uvedeno srovnání ceny elektřiny v zemích Evropy.

Tabulka 2-1: Ceny elektřiny v Evropě

Ceny elektřiny za 1 MWH k 1. polovině roku 2017								
Nízkás potřeba			Střední spotřeba			Velká spotřeba		
Pořadí	země	Cena v €	Pořadí	země	Cena v €	Pořadí	země	Cena v €
1	Německo	336	1	Dánsko	305	1	Německo	288
2	Dánsko	329	2	Německo	305	2	Belgie	253
3	Belgie	310	3	Belgie	280	3	Dánsko	240
4	Irsko	298	4	Irsko	231	4	Itálie	224
5	Spanělsko	286	5	Spanělsko	230	5	Portugalsko	219
6	Portugalsko	250	6	Portugalsko	228	6	Řecko	208
7	Norsko	248	7	Itálie	214	7	Spanělsko	193
8	Rakousko	243	14	Francie	169	11	Rakousko	171
16	ČR	191	22	ČR	144	23	Slovensko	122
21	Slovensko	170	23	Slovensko	144	27	ČR	114
40	Ukrajina	39	40	Ukrajina	39	40	Ukrajina	39

Zdroj: www.elektrina.cz

Jak je vidět z tabulky 2-1, je cena elektřiny v České republice relativně nízká v porovnání s ostatními zeměmi EU. Nejdražší elektřina je v zemích jako Německo, Dánsko a Belgie. Nejnižší je naopak na Ukrajině, kde činí 39 € za jednu megawatthodinu.

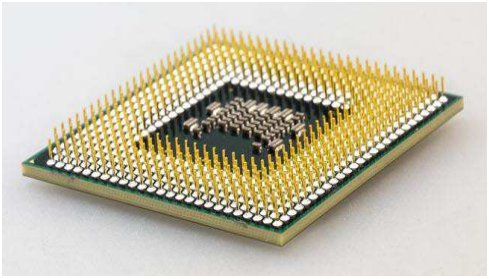
Protože těžící přístroje bývají zpravidla velmi výkonné a energeticky náročné, vzniká mnoho odpadního tepla, které je potřeba regulovat. Dalším nákladem proto většinou bývá také nákup chlazení, jež není ovšem podmínkou. Je též možné teplo vzniklé při těžbě smysluplně využít například k ohřevu bazénu či jiných věcí, přičemž v mnoha případech lze z vytápění generovat relativně velké výnosy. Všechny tyto náklady a jejich možná optimalizace

v konečném důsledku ovlivňují ziskovost těžby. V práci bude počítáno s náklady počátečními a náklady na elektřinu, přičemž s možnými výnosy z prodeje tepla nebude počítáno, neboť relevantní výpočet je v podmínkách teoretické koncepce práce prakticky nemožný.

2.4.3 **Způsoby těžby**

Z počátku se bitcoin těžil individuální cestou. První nadšenci z řad pokračovatelů projektu Sathosiho Nakamota napomáhali k rozvoji bitcoinové sítě, což zahrnovalo také těžení za účelem vytvoření prvních bloků bitcoinů. To znamenalo, že si těžař nakoupil nástroje k těžbě (pokud už zařízení neměl), zaktivoval potřebný software a nechal počítač provádět složité výkony, které po určitém čase přinesly kýžený obnos v podobě konkrétního počtu bitcoinů. V prvopočátku byla těžba relativně jednoduchá a k získání bloku stačilo využít osobní počítač. Těžba probíhala využitím výkonu procesoru (CPU) v počítači, přičemž v prvopočátcích takto bylo možné vytěžit stovky bitcoinů v průběhu jednoho týdne.

Obr. 2-9: Vzhled procesoru



Zdroj: www.tech.summizary.com

Ovšem s tím jak se bitcoin stával stále více populární a jeho cena rostla, přibývalo těžařů jak z řad kryptonadšenců, tak i z řad investorů nebo zkrátka lidí hledající alternativní investice k svému portfoliu finančních nástrojů. Větší počet těžařů však výrazně ztížil těžbu a prakticky udělal z těžby na osobním počítači prodělávající činnost.

Na scénu se dostaly grafické karty, s jejichž využitím k těžbe bitcoinů přišel bitcoinový nadšenec Laszlo Hanecz. S tím, jak každý na síti využíval ke generovámí bloků CPU a cena bitcoinu v té době byla nízka, nevyplatilo by se nakupovat více počítačů za účelem těžby. Laszlo rozuměl počítačům natolik aby věděl, že procesor mimo výpočtu funkcí náležících k těžbě, slouží také k zajištění chodu jiných procesů v počítači a není tak těžebně stoprocentně efektivní. Naproti tomu GPU (grafický procesor) je na míru vytvořen k řešení opakujících se problémů důležitých k zpracování obrazu a videa. Laszlo také přišel s tím, jak naprogramovat

GPU k těžbě, čímž namísto 50 bitcoinů za jeden den, které ztěží získával využitím CPU, vytěžil v průběhu jedné hodiny bitcoinů 50 až 100.

Obr. 2-10: Druhy grafických karet

Zdroj: www.argyllfreepress.com

Využívání grafických karet opět udělalo těžbu výnosnou, nicméně s rostoucím počtem těžařů pomocí grafických karet nebyli dodavatelé grafických karet schopni situaci na trhu zvládnout a některé výkonné grafické karty se staly nedostatkovým zbožím a rostly tak počáteční náklady na pořízení těchto karet. Navíc s rostoucím počtem uživatelů grafických karet k těžbě opět narůstal výpočetní výkon celé sítě, což mělo podobný scénář jako v případě užívání stolních počítačů. Bylo potřeba znovu přijít s něčím, co by posunulo efektivnost těžby směrem nahoru a zlepšilo finanční výsledky těžařů.

A tehdy se začaly využívat konfigurovatelné integrované obvody – hradlová pole (FPGA), jež lze naprogramovat pro řešení specifické úlohy. Jelikož je FPGA levnější a mnohem výkonnější než GPU (grafické karty), došlo k zefektivnění těžby až na desetinásobnou hodnotu. Ovšem opravdovou změnu přinesly až specializované integrované obvody (ASIC), které jsou v rámci zařízení specializovaných na těžbu bitcoinů navrženy k řešení úloh vedoucích k nalezení bloku. Ačkoli je ASIC čip výrazně dražší než GPU, dosahuje nesrovnatelného výkonu při relativně nízké spotřebě elektřiny. Z několika stovek MH/s, typických pro grafické karty, se těžba pomocí ASIC dostala až na úroveň několika milionů MH/s na jeden přístroj. Zařízení využívající specializované integrované obvody je znázorněné na obrázku 2-11. Jedná se o Antminer S9.

Obr. 2-11: Antminer S9

Zdroj: www.ricardo.ch

Přesto je dnes velmi obtížné těžit, zejména bitcoin, jako samostatná entita. Pokud není těžař ochoten investovat do těžebních zařízení vysoké částky, je v podstatě nemožné na bitcoinu vydělat. Obtížnost celé sítě a velikost výpočetního výkonu odsuzuje výpočetně malého těžaře k nezdaru. Důvodem je zejména dlouhá doba k nalezení bloku, jež může samostatnému těžaři trvat i několik let, zdali vůbec. Těžař sám si může dobu potřebnou k nalezení bloku na základě výpočetní síly svých zařízení spočítat takto:

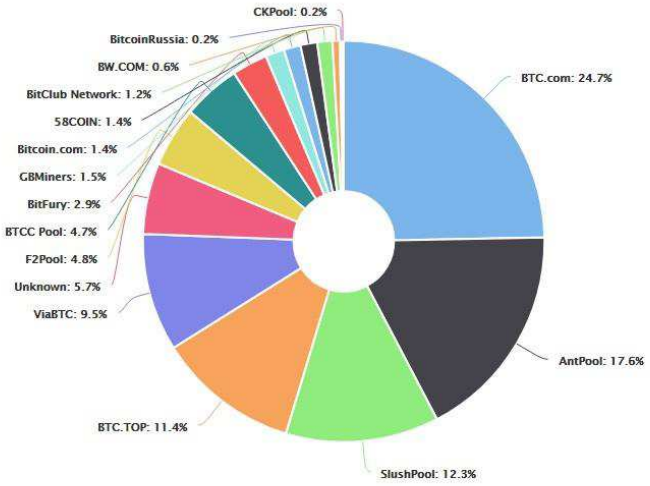
$$\check{c}as = \frac{obtížnost \cdot 2^{32}}{hash\ rate}. \qquad (2.1)$$

Jak se lze přesvědčit provedením výpočtu dle vzorce (2.1),samotnému těžaři by za využití výpočetní síly 27 000 GH/s trvalo více než 13 let k nalezení jednoho bloku. Aby těžař nalezl při obtížnosti o velikosti 2 603 077 300 218 blok alespoň jednou za měsíc, musela by jím dosažená výpočetní síla odpovídat hodnotě 4.31 PH/s.

Protože je velmi obtížné inkasovat bitcoiny v individuální těžbě, vznikly v rámci bitcoinové sítě tzv. ***těžařské pooly***. Jedná se vlastně o obdobu investičních fondů, které umožňují i méně movitým jedincům podílet se na výnosech obrovského portfolia produktů, jež by sami nikdy nebyli schopni získat. Na základě vložené procentní částky vůči celku poté inkasují odměnu. Stejně je tomu v rámci těžby bitcoinů. Těžař se určitým procentem podílí na těžbě bitcoinu v rámci poolu a získává odměnu, jež je přímo úměrná procentu výpočetnímu výkonu, který dodává celému poolu. Výhodou je to, že inkasuje odměny pravidelně, neboť pooly se výrazně podílejí na výpočetním výkonu celé sítě a inkasují tak odměny pravidelně.

Každý těžební pool má stanoveny vlastní mechanismy výpočtu odměny a velikosti poplatků. Analogie zmíněná výše je pouze jednoduchým přirovnáním skutečnost, protože výpočty odměny nejsou závislé pouze na výpočetním výkonu jako takovém, ale i na dalších důležitých faktorech[6]. Níže uvedený obr. 2-12 zobrazuje jednotlivé těžební pooly a jejich zastoupení na výpočetním výkonu celé sítě.

Obr. 2-12: Procentní zastoupení těžebních poolů na celkovém výpočetním výkonu poolů



Zdroj:www. blockchain.info

Ze čtyř největších poolů jsou právě tři pooly registrované a spravované v Číně, přičemž podíl čínských těžících poolů je na celkovém výpočetním výkonu roven cca 81 %. Mezi první desítkou a v obrázku 2-10, vztahujícím se k prvnímu únoru 2018, na třetím místě je Slushpool, původem z České republiky.

Posledně zmíněným způsobem těžby je tzv. ***cloud mining***. Princip tohoto způsobu těžby spočívá ve vzdáleném pronajmutí výpočetního výkonu u určitého dodavatele. Odpadá tedy potřeba nakoupit těžební přístroj, jeho údržba a veškeré věci s tím spojené. Po nakoupení výpočetního výkonu poté investor pouze inkasuje zisky, tedy pokud jsou nějaké. Nicméně je potřeba dobře prozkoumat trh těchto věcí a bezpečnost jednotlivých společností, neboť se mnohdy stává, že na pozadí údajných těžebních farem stojí podvodníci a investor tak může přijít o celou částku, bez možnosti zpětné kompenzace.

[6] Odkaz: https://slushpool.com/help/manual/rewards

2.4.4 **Slush pool**

Detailnějšímu popisu následujícího těžebního poolu bude věnována pozornost z důvodu výběru tohoto poolu v rámci těžby. Výběr právě tohoto poolu je podepřen následujícími fakty. Jedná se o první pool na těžení bitcoinů, jenž byl založen občanem České republiky Markem Palatinem. V rámci Slush poolu bylo od roku 2010 vytěženo přes milion bitcoinů, které byly stabilně a přesně vypláceny po celou tuto dobu. Infrastruktura běží na vysoce bezpečných serverech a výplatní adresa může být zabezpečena dvoufaktorovou autentizací. Výpočetním výkonem se řadí do první desítky nejvýkonnějších poolů, a ačkoli není výpočetně nejsilnější, tak je pravděpodobně jeden z nejlepších a nejpopulárnějších poolů na světě.

Výpočet odměny za nalezený blok je specifický pro každý těžební pool zvlášť, nicméně každý vychází z podobné myšlenky proporcionálního rozdělení odměny na základě poměru výkonu k celku. To co pooly odlišuje je zejména výše poplatku a matematika schovaná v pozadí výpočtu odměn.

U Slush poolu je základem pro výpočet odměny vyměřený skórovací hash rate těžaře, jež je dán do podílu vůči hash rate celého poolu. Skórovací hash rate je ve své podstatě exponenciální klouzavý průměr hash rate veškerých zařízení uživatele připojených k danému poolu. Protože se jedná o klouzavý průměr, jsou vyhlazeny krátké propady a nárůsty hash rate, což napomáhá lepšímu rozdělení odměn v rámci poolu. Pro výpočet odměn se využívá hash rate z času nalezení konkrétního bloku.

Odměna je tedy zjednodušeně počítána dle následujícího vzorce:

$$y = hodnota\ bloku \cdot (1-p) \cdot \frac{SHRT}{SHRP}. \tag{2.2}$$

kde y značí odměnu, p demonstruje poplatek poolu (2%), $SHRT$ je skórovací hash rate těžaře a $SHRP$ znamená skórovací hash rate poolu.

Hodnota bloku činí 12.5 bitcoinů, přičemž jsou nad výši této odměny započítány také transakční poplatky z transakcí zapsaných v daném bloku. Počet bitcoinů získaných z bloku ovšem není stálý, neboť v průběhu času dochází k tzv. půlení odměn. Další půlení s největší pravděpodobností nastane počátkem roku 2021 a sníží tak odměnu na 6.25 bitcoinů za každý blok.

V práci bude využíván zjednodušený princip, kdy bude předpokládán stabilní skórovací hash rate ve výši hash rate udávaného výrobcem jednotlivých těžících zařízení. Ve skutečnosti však stabilní není, neboť se mění například s tím, jak vypínáme a zapínáme těžbu. Obr. 2-13 demonstruje rozdíl mezi efektivním a dosaženým hash rate po začátku a konci těžby. Z obrázku 2-13 je patrné, že efektivní hash rate (modrá čára) je po začátku těžby v 9:30 vyšší, než skórovací. Naopak po vypnutí těžby klesá efektivní mnohem rychleji, což znamená, že ještě chvíli po ukončení těžba probíhá, čímž se navyšuje celkový skórovací hash rate. To a mnohem více věcí v praxi ovlivňuje celkovou odměnu odvozenou právě ze skórovacího hash rate. Vzhledem k vysoké obtížnosti a dost možná i praktické nemožnosti predikce skórovacího hash rate, proto bude využito výše zmíněného zjednodušujícího principu.

Obr. 2-13: Efektivní a skutečný hash rate

Zdroj: www.slushpool.com

V rámci zmíněného zjednodušení lze výpočítat pravděpodobnost získání odměny jako podíl výpočetního výkonu (H/s) těžaře a celkového výpočetního výkonu bitcoinové sítě. Výpočet celkové výše odměny je možné počítat pro různé časové intervaly. V práci je výpočet odměny počítán měsíčně dle tohoto vztahu:

$$y = \frac{Hash\ rate}{Celkový\ hash\ rate} \cdot 5400, \tag{2.3}$$

kde *Hash rate* značí výpočetní výkon těžaře, *Celkový hash rate* je výpočetní výkon celé sítě a 5 400 značí celkové množství vytěžených bitcoinů všemi těžaři za jeden měsíc při výši odměny 12.5 BTC.

3 Teoretická východiska a popis metodiky

Třetí kapitola je zaměřena na popis metodiky, jež je využita v práci k predikování hodnot a komputaci důležitých výpočtů vedoucích k cíli práce. Jako první bude popsán princip simulací náhodného vývoje finančního aktiva, jež využívá geometrický Brownův pohyb. Dále je stručně popsána simulace rozdělení pravděpodobnosti náhodného vývoje ceny finančního instrumentu, vedená skrze simulaci Monte Carlo. Následuje popis investičního rozhodování, v rámci nehož jsou uvedeny jednotlivé fáze projektu, způsoby financování a nástroje určené k hodnocení efektivnosti projektů. Kapitola je zakončena popisem nákladů na kapitál a kritérií hodnocení projektů.

3.1 Finanční modelování

Finance umožňují efektivní regulaci a řízení ekonomických a finančních systémů, navíc jsou též nástrojem pro rozhodování samostatných ekonomických subjektů a institucí. Finanční instrumenty, a finance obecně, je možné považovat za jedny z elementárních prostředků umožňujících sledovat, zachytit, vyjádřit a řídit finanční a ekonomické činnosti. V rámci současné ekonomiky dochází k stále zřetelnějšímu propojování aktivit a procesů, které tvoří entitu zvanou ekonomický nebo finanční systém. V průběhu času je proto stále obtížnější, jak pro malého podnikatele, tak i pro nadnárodní společnosti, rozhodování na poli záležitostí týkajících se finančních a ekonomických problémů.

S rostoucí obtížností a rizikovostí rozhodování dochází k systematickému vylepšování či tvorbě metodologie vedoucí ke zkvalitnění procesů finančního rozhodování. Nejde ovšem o prostředky, které lze využívat slepě a automaticky. Tyto prostředky je nutné kriticky příjmout a správně aplikovat s ohledem na předpoklady, na jejichž základě byly vytvořeny a formulovány.

Jeden z rychle se rozvíjejích finančních nástrojů, který napomáhá subjektům ke zkvalitnění finančního rozhodování a tvorbě finančních plánů do budoucna, je finanční modelování. Finanční modelování reprezentuje souhrnné zpracování finanční problematiky od zaměření věcného až po aplikaci sofistikovaných matematických prostředků. V procesu samotného modelování je využito širokého spektra nástrojů a informací z oborů ekonomických, matematických nebo statistických.

Jak uvádí Zmeškal a kol (2013) finančním modelům je potřeba rozumět jako nástrojům, jež mohou napomoci v procesu finančního rozhodování, nicméně rozhodujícím subjektem je pokaždé člověk. V případě, kdy model nevede k vhodným výsledkům, není možné poukazovat na chybovost modelu, nýbrž je nasnadě hledat chybu u konkrétního subjektu, který model nesprávně použil. Následně se s velkou pravděpodobností jako příčina ukáže nerespektování základních předpokladů a podmínek modelů. Je tudíž důležité finančním modelům správně porozumět a dokázat výsledky vhodně aplikovat. Jakmile dokáže subjekt finanční modely adekvátně využít, má k dispozici kvalitní nástroj k snížení rizik a zkvalitnění rozhodovacích procesů vedoucích k udržení tržního postavení nebo jeho zlepšení.

Finanční modely lze členit a charakterizovat na základě velkého množství kritérií, například dle finanční aplikace nebo rozhodovacího prostředí a podmínek. Možná rozdělení lze najít například v knize Finanční modely (Zmeškal a kol., 2013), ze které je následující text čerpán.

Při finančním modelování je důležité dodržovat jasně stanovený postup. Je potřeba si ujasnit jednotlivé kroky celého procesu a jejich logickou návaznost. Postup je možné rozdělit do těchto fází (Zmeškal a kol., 2013):

- Slovní definování problému.
- Matematická formulace finančního modelu (optimalizační, simulační nebo ekonometrické modely).
- Opatření výchozích dat (může se jednat o tržní data nebo parametry stanovené finančním analytikem).
- Transformace tržních dat (v této fázi jsou tržní data transformována na vyžadované vstupní paramtery modelů pomocí predikčních modelů nebo provedením transformace k získání vstupních dat, jež nejsou dostupná přímo).
- Tržní data je důležité testovat také statisticky. Testovány jsou statistické předpoklady a statistická spolehlivost vstupních dat (v této fázi dochází například k eliminaci multikolinearity časových řad).
- Řešení úloh pomocí prostředků matematického modelování (lze využít modulů Excelu nebo aplikovat profesionální software).
- Interpretace dosažených výsledků a formulace námětů pro další analýzy (prověření citlivosti výsledků).

Využití finančního modelování je velmi rozsáhlé a lze ho využívat k vytvoření různých druhů portfolií splňujících uživatelem definované vlastnosti, k oceňování opcí nebo k tvorbě dlouhodobých finančních modelů firmy. V následujícím textu je detailněji popsán a vysvětlen princip simulace náhodného vývoje ceny finančního intrumentu včetně rozdělení pravděpodobnosti na základě geometrického Brownova pohybu, neboť se jedná o metody, jež jsou v práci využita k predikci ceny a výpočetního výkonu bitcoinové sítě.

3.1.1 Simulace náhodného vývoje ceny finančního instrumentu

V procesu simulace náhodného vývoje je využíváno například generátoru pseudonáhodných čísel v Excelu pro generování náhodných čísel z vybraných rozdělení pravděpodobností, jež jsou užity jako vstupy rovnic sloužících k výpočtu budoucích cen. Jak uvádí Zmeškal a kol. (2013) nelze považovat tento generátor za generátor zaručující profesionální kvalitu, přesto lze výsledky na tomto postupu založené považovat za dobré a věrohodné. V případě, že není k dispozici požadované rozdělení pravděpodobnosti, lze jej získat pomocí procedury inverzní transformace.

Jak uvádí Zmeškal a kol. (2013), vychází se z vlastnosti distribučních funkcí, jež jsou neklesající funkce, čímž existuje vzájemně jednoznačné přiřazení mezi náhodnými čísly rovnoměrného rozdělení z intervalu [0,1] a distribuční funkcí. Obecně tudíž $x = F^{-1}(r)$, kde $x \in [a,b]$ reprezentují náhodná čísla z distribuční funkce F a r reprezentují náhodná čísla z rovnoměrného rozdělení pravděpodobnosti. To protože $F(x) = G(r)$, tudíž $x = F^{-1}[G(r)]$, a také protože pro rovnoměrné rozdělení v intervalu [0,1] platí $G(r) = r$.

Finanční aktiva jsou charakteristické tím, že jejich vývoj je v čase náhodný, tedy stochastický. Tento proces je možné v zásadě popsat diskrétně s aplikacemi při simulacích nebo při analytickém řešení spojitě. Klíčové pojmy v této souvislosti tvoří zejména Wienerův proces, Itôův proces, Itôova lemma a geometrický Brownův proces. Dle Zmeškal a kol. (2013) vychází Wienerův proces ze dvou předpokladů:

- změny cen jsou nezávislé v čase,
- sleduje Markovův proces, což znamená, že predikované ceny jsou ovlivněny pouze aktuální cenou, nikoliv cenami historickými.

Wienerův proces je definován následovně,

$$\widetilde{z}_{0+dt} - z_0 = dz = \widetilde{\varepsilon} \cdot \sqrt{dt} \tag{3.1}$$

kde dt stojí pro nekonečně malou změnu času a $\widetilde{\varepsilon}$ symbolizuje náhodnou proměnnou z normovaného normálního rozdělení N (0,1). To znamená, že střední hodnota je nulová a rozptyl odpovídá časové změně, $\text{var}(dz) = dt$, přičemž její odmocninou je směrodatná odchylka, $\sigma(dz) = \sqrt{dt}$. Celková změna času je tedy *T*.

V případě, že uvažujeme vývoj ceny v čase za počtu intervalů k o stejné délce dt, potom:

$$\widetilde{z}_T - z_0 = \sum_{i=1}^{k} \widetilde{\varepsilon}_i \cdot \sqrt{dt} \tag{3.2}$$

Z čehož lze odvodit, že

$$E(\widetilde{z}_T) = 0, \quad \text{var}(\widetilde{z}_t) = k \cdot dt = T \quad a \quad \sigma(\widetilde{z}_T) = \sqrt{T}. \tag{3.3}$$

Jeden z obecných druhů stochastických procesů se nazývá Itôův proces. Jedná se o proces, který jako zvláštní případy zahrnuje Wienerovy procesy, a který je pro proměnnou *x* definován takto:

$$dx = a(x;t) \cdot dt + b(x;t) \cdot dz \tag{3.4}$$

kde je $a(\cdot)$ značí přírůstek a $b(\cdot)$ je volatilia změny proměnné.

Pro nestochastické funkce je definován Taylorův rozvoj, což je matematický postup, v rámci něhož dochází k nahrazení funkce nekonečně dlouhou mocninnou řadou. V praktickém užití se využívá Taylorův rozvoj pouze do určitého stupně rozvoje, přičemž vyššímu stupni rozvoje odpovídá lepší přiblížení zvolené funkce. Z hlediska funkcí jejichž proměnnými jsou procesy stochastické dle (3.4) a čas se využívá Itôova lemma, $G = f(x,t)$. Zmíněná funkce je definována následujícím způsobem:

$$dG = \left[\left(\frac{\partial G}{\partial x} \cdot a(\cdot) \right) + \frac{\partial G}{\partial t} + \frac{1}{2} \cdot \frac{\partial^2 G}{\partial x^2} \cdot b^2(\cdot) \right] \cdot dt + \frac{\partial G}{\partial x} \cdot b(\cdot) \cdot dz. \tag{3.5}$$

Daná funkce je Itôovým procesem, přičemž přírůstek je vyjádřen v hranatých závorkách,

$$\frac{\partial G}{\partial x} \cdot a\,(\cdot) + \frac{1}{2} \cdot \frac{\partial^2 G}{\partial x^2} \cdot b^2\,(\cdot) + \frac{\partial G}{\partial t}, \tag{3.6}$$

a rozptyl je dán tímto vztahem:

$$\left(\frac{\partial G}{\partial x}\right)^2 \cdot b(\cdot). \tag{3.7}$$

Zvláštním případem obecného Itôova procesu je aritmetický Brownův pohyb, jež bývá také nazýván jako zobecněný Wienerův proces:

$$dx = \mu \cdot dt + \sigma \cdot dz. \tag{3.8}$$

Jde o Itôův proces s konstatními parametry, které jsou nezávislé na ostatních proměnných. Cena se tedy vyvíjí lineárním trendem:

$$E(dx) = \mu \cdot dt, \quad E(x_T) = x_0 + \mu \cdot T, \quad \text{var}(dx) = \sigma^2 \cdot dt, \quad \text{var}(x_T) = \sigma^2 \cdot T. \tag{3.9}$$

Dalším případem tohoto obecného procesu je geometrický Brownův pohyb, jež má nemalé uplatnění ve finančním modelování a v rámci něhož se cena vyvíjí exponenciálním trendem. Geometrický Brownův pohyb vychází z následující formulace:

$$dx = \mu \cdot x \cdot dt + \mu \cdot x \cdot dz, \tag{3.10}$$

Aby byla zřejmá interpretace parametrů a celého procesu, lze uvedený vzorec (3.10) zapsat i takto:

$$\frac{dx}{x} = \mu \cdot dt + \sigma \cdot dz. \tag{3.11}$$

Z toho je patrné, že je daný proces vhodný pro definování výnosu ceny aktiva *x*, kde μ značí průměrný výnos aktiva, nejčastěji za jeden rok, a σ směrodatnou odchylku aktiva *x*, také nejčastěji za období jednoho roku. Střední hodnotu a rozptyl je možné stanovit takto:

$$E(dx) = \mu \cdot dt, \quad \text{var}(dx) = \sigma^2 \cdot dt, \tag{3.12}$$

Pokud předpokládáme, že se výnos finančního aktiva vyvíjí na základě procesu popsaného v (3.10), pak lze s užitím Itôovy lemmy pro funkci (G = ln *x*) ukázat, že

$$dG = d\ln S = \alpha \cdot dt + \sigma \cdot dz. \tag{3.13}$$

Nyní jde o vyjádření spojitého výnosu, kde $\alpha = \mu - \frac{\sigma^2}{2}$ a $\mu = \ln \frac{S_T}{S}$.. Pro finanční aktivum *S* lze postupně odvodit budoucí cenu:

$$S_T = S_0 \cdot \exp(\alpha \cdot T + \sigma \cdot z), \tag{3.14}$$

očekávánou budoucí cenu:

$$E(S_T) = S_0 \cdot \exp(\mu \cdot T) \tag{3.15}$$

a rozptyl:

$$\text{var}(S_T) = S^2 \cdot \exp(2 \cdot \alpha \cdot T) \cdot \left[\exp(\sigma^2 \cdot T) - 1\right] \tag{3.16}$$

Nyní lze určit hodnotu kvantilu log-normálního rozdělení na dané hladině pravděpodobnosti γ, který definuje očekávanou budoucí cenu s užitím funkce inverzní k distribuční funkci normovaného normálního rozdělení Φ:

$$S_T^{\gamma} = S_0 \cdot \exp(\alpha \cdot T + \Phi^{-1}(\gamma) \cdot \sigma \cdot \sqrt{T}). \tag{3.17}$$

3.1.2 Simulace rozdělení pravděpodobnosti náhodného vývoje ceny bitcoinu

K simulaci rozdělení pravděpodobnosti náhodného vývoje ceny bitcoinu a hash rate je využívána metoda Monte Carlo, přičemž se cena bitcoinu vyvíjí podle geometrického Brownova pohybu. Metoda Monte Carlo je nástrojem řešení pravděpodobnostních modelů, jež je obtížné řešit analyticky. Simulace Monte Carlo využívá zákona velkých čísel, který demonstruje skutečnost, že se zvyšujícím se počtem nezávislých opakovaných pokusů k sobě konvergují teoretické a empirické (popisované výsledky provedených pokusů) charakteristiky. Při dostatečně velkém množství pokusů *n* je možné odhadnout střední hodnotu $E(Xn)$, přičemž platí, že při velkém počtu nezávislých pokusů je aritmetický průměr výsledků jednotlivých pokusů vzdálen od střední hodnoty jen velmi málo. V praxi je relativně obtížné získat výsledky vysokého počtu realizací náhodných proměnných, a proto je využíváno umělého vytváření náhodných pokusů. Postup provedení metody Monte Carlo v této je následující:

- První krokem je vygenerování náhodných čísel z normovaného normálního rozdělení N(0;1) za pomocí funkce v programu Excel – Generátor pseudonáhodných čísel. V souvislosti s požadovaným množstvím kroků simulace a počtem simulovaných scénářů je potřeba také zvolit konkrétní hodnoty pro tyto veličiny.
- Druhým krokem je dosazení potřebných hodnot do vztahu dle (3.17) a za pomocí relativního kopírování jsou generovány náhodné ceny aktiva. Následně je nutné tyto hodnoty vhodným způsobem prezentovat, k čemuž jsou využity další funkce programu Excel. Za účelem zjištění rozdělení pravděpodobnosti ceny aktiva je možné využít funkce ČETNOSTI (FREQUENCY), kde vstupními agrumenty jsou výsledné ceny aktiva a meze intervalů, pro které je zjišťován absolutní počet scénářů v daném intervalu.

Cena dle (3.14) je pro jednotlivé scénáře j formulována následovně:

$$S_{t+\Delta t}^{(j)} = S_t^{(j)} \cdot \exp\left[\left(\mu - \sigma^2/2\right)\cdot \Delta t + \sigma \cdot \tilde{\varepsilon}_t^{(j)} \cdot \sqrt{\Delta}\right] \tag{3.18}$$

3.2 Investiční rozhodování

Investiční rozhodování je velmi významným druhem rozhodnutí, jak na úrovni podniku, tak i na úrovni jednotlivce. Význam spočívá hlavně v důsledcích investičních rozhodnutí, které působí dlouhodobě a při špatné volbě investičního projektu mohou znamenat též vysoké ztráty. Dlouhodobá rozhodnutí probíhájí za podmínek rizika a nejistoty, neboť není předem znám budoucí vývoj a zvolený scénář závisí na mnohých faktorech a okolnostech, které jsou zcela náhodné. Proto je potřeba využívat, v začátku i průběžně, veškerá dostupná data a nástroje, které napomohou rozhodovateli ke snížení možných rizik a následně možných ztrát.

Dle Dluhošové (2010) lze investiční projekty různě klasifikovat například z hlediska časového nebo způsobu financování. Dále jsou uvedeny některá členění, jež mohou být použity i v případě individuální investice, jakou je kupříkladu investice do těžících zařízení jednotlivcem.

1. **Členení z hlediska účetnictví**

- Finanční investice – jde o nákup finančních instrumentů jako jsou akcie, obligace nebo podílové listy.
- Hmotné investice – hmoutnou investicí může být nákup stroje, budovy nebo pozemků za účelem využívání k produkci statků či služeb.

- Nehmotné investice – nákup softwaru, know-how nebo licencí.

2. Dle způsobu financování

- Nezadlužený projekt – financován převážně z vlastních zdrojů.
- Zadlužený projekt – zdroje k financování tvoří mimo vlastních zdrojů také zdroje cizí (bankovní úvěr, emise dluhopisů podnikem).

3. Dle typu peněžního toku

- Konvenční –jedná se o takový projekt, kdy po úvodním období kapitálových výdajů následuje období s převahou příjmů z investice.
- Nekonvenční – po počátečních kapitálových výdajích je potřeba s postupem času vynaložit další výdaje, například na údržbu zařízení.

4. Dle doby výstavby

- Jednoleté projekty – doba výstavby je kratší než jeden rok.
- Víceleté projekty - výstavba investičního zařízení trvá déle než jeden rok.

5. Dle možnosti zásahů v budoucnu

- Aktivní investice – dochází k vyhodnocení realizace aktivních zásahů jakými jsou rozšíření, zůžení nebo zastavení projektu.
- Pasivní investice – aktivní zásahy v době investice se neuvažují.

3.2.1 Fáze investičního projektu

Realizaci investičního projektu je možné shrnout do několika fází, které odlišuje jednak časový horizont, a jednak věcná náplň těchto fází. Dle Dluhošové (2010), jsou fáze investičního projektu následující:

- předinvestiční fáze,
- investiční fáze,
- provozní fáze,
- ukončení a likvidace projektu.

Fáze předinvestiční je základem kvalitní realizace a úspěšnosti projektu, neboť právě v této fázi jsou zkoumána a učiněna zásadní rozhodnutí. Předinvestiční fáze zpravidla zahrnuje několik na sebe navazujících etap.

První etapou je *identifikace projektu*, kdy dochází ke zpracování dostupných informací o podnikatelských příležitostech. Seznámení se s možnými podnikatelskými příležitostmi předchází získávání důležitých podnětů z okolí, které zahrnuje zkoumání podnikatelského

přostředí a možných investičních příležitostí. Výsledkem této etapy je vyhodnocení různých možností v rámci investování a vytvoření portfolia projektů, jež se jeví jako zajímavé a efektivní.

Druhou etapou je *průběžný výběr* projektů, které je možné považovat za uskutečnitelné a z hlediska ziskovosti za proveditelné. Výstupem této etapy tak bývá předběžné zpracování *technicko-ekonomické studie,* jež je mezistupeň předcházející samotný výběr investičního projektu. Technicko-ekonomická studie představuje detailní zpracování projektu, které by mělo poskytnout podklady a informace potřebné pro rozhodnutí o realizaci konkrétního investičního projektu. Celá studie vychází z detailního průzkumu podmínek panujících na konkrétní trhu a důkladné prognozy tohoto trhu spolu s provedením analýzy podnikových možností. Detailní finančně-ekonomická analýza se zpracovává v několika scénářích a podílí se na ní skupina odborníků ze všech důležitých oblastí. Jestliže je nalezen určitý problém z hlediska proveditelnosti nebo ziskovosti projektu, je tento projekt zamítnut. V případě samotného zamítnutí je poté potřeba průběžně zkoumat nové příležiosti na trhu a jejich možnou realizaci.

Jestliže je některý z možných projektů vybrán jako proveditelný, nastává ***fáze investiční*** v rámci níž dochází k samotné realizaci projektu od zádání až do jeho uvedení v provoz. Elementární etapy této fáze tvoří jednak zpracování úvodní projektové dokumentace, tak zpracování realizační projektové dokumentace a rozhodnutí o zahájení výstavby projektu a jeho realizace. Následuje zkušební provoz a samotné uvedení do provozu.

Ve ***fázi provozní*** jsou generovány jednotlivé finanční toky, jejichž stabilita a výše oproti prvotním výdajům rozhoduje o ekonomické efektivnosti investice a její ziskovosti. Je zřejmé, že ziskovost a efektivnost značně závísí na kvalitě zpracování projektu ve fázi předinvestiční a technicko-ekonomické studie.

Fáze ukončení a likvidace je závěrečnou fázi živostnosti projektu a zahrnuje zastavení samotné výroby a veškeré činnosti spojené s ukončením. Mezi činnosti spojené s ukončením investice patří prodej likvidovaného majetku spolu s jeho demontáží a prodejem přebytečných zásob. Rozdíl mezi příjmem a výdaji na prodej likvidovaného majektu představuje likvidační hodnotu, jež je součástí peněžního toku v posledním období životnosti projektu. Může ovšem nastat situace, kdy zařízení není možné prodat a příjem z likvidace je proto roven nule.

3.2.2 **Financování investic**

Mimo rozhodnutí o realizaci konkrétního projektu, je potřeba rozhodnout o způsobu jeho financování. Výběr druhu financování ovlivňuje ziskovost projektu a je proto důležitou součástí celkového investičního procesu. Struktura financování by měla být zvolena tak, aby náklady na vynaložené zdroje byly minimální a byla zajištěna stabilita přílivu peněžních prostředků.

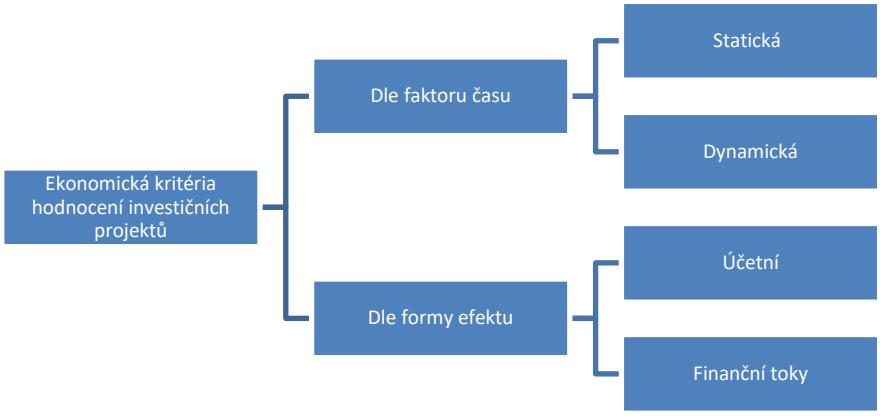
V podstatě je veškeré rozhodování zaměřeno na otázku, zdali projekt financovat z vlastních nebo cizích zdrojů. Jestliže je projekt financován pouze vlastními zdroji, jedná se o tzv. samofinancování. Při samofinancování je velkou výhodou, že nevznikají náklady na cizí kapitál a nezvyšuje se stupeň zadlužení subjektu. Jedná se ale o dražší a potenciálně nestabilní zdroj financování. Alternativou samofinancování je financování za pomocí cizích zdrojů. Hlavním zdrojem bývají zpravidla bankovní úvěry, jejichž získání je spojené s řadou podmínek, které subjekt musí splnit, například zpracování podnikatelského záměru. Subjekt musí obvykle sdělit účel půjčky a předložit potřebné informace, na základě kterých věřitel určí, zdali bude úvěr poskytnut a za jakých podmínek. Zvolené podmínky, tedy způsob splácení, zajištění úvěru a výše úrokové sazby, následně rozhodují o efektivnosti investice a jeho potenciální ziskovosti.

3.2.3 **Hodnocení investičních projektů**

K rozhodnutí o realizaci konkrétního projektu se využívá celá řada kritérií hodnocení investic. Princip spočívá v porovnání výdajů, které je nezbytné vynaložit na projekt a ekonomických efektů, které realizací vzniknou. Důležitým předpokladem správného vyhodnocení projektů je vymezení předmětu, který je hodnocen, tedy definice hranic systémů výstupů a vstupů, prostředků a zdrojů investičního celku. Je potřebné také stanovit srovnávací základny hodnocení, aby bylo možné hodnotit rozličné investiční projekty. Taktéž je nutné určit moment, ke kterému je vyhodnocení vztaženo, přičemž z praktických důvodů je nejčastěji zvolen rok uvedení investice do provozu. Hodnocení projektů vychází z porovnání výchozího a cílového stavu, kdy je srovnán stav v případě nerealizace projektu a konečný stav s dopady realizace investice.

Jednotlivá kritéria lze členit podle různých aspektů. Dluhošová (2010) ve své knize uvádí členění dle faktoru času a dle formy ekonomického efektu projektu. Toto členění shrnuje obrázek 3-1.

Obr. 3-1: Rozdělení ekonomických kritérií hodnocení investičních projektů



Zdroj: Dluhošová (2010)

Rozdílnost kritérií v závislosti na faktoru času spočívá v jeho zohlednění u dynamických kritérií a nezohlednění u kritérií statických. Zohlednění faktoru času u kritérií dynamických spočívá v diskontování budoucích příjmů a výdajů z investičních projektů. V případě statických kritérií se vychází z nominálních hodnot.

Efektem při zvolení účetních kritérií jsou veličiny jako náklady a zisk a základem jsou data z výkazu zisku a ztráty. U kritérií založených na nákladovém přístupu je výsledným efektem, kte kterému je vztaženo rozhodnutí o realizaci, zpravidla úspora nákladů. Z hlediska ziskových kritérií je tímto efektem výsledný zisk, tedy některá z variant vyjádření zisku (čistý zisk, hrubý zisk, EBT). Využití účetních efektů doprovází řada nedostatků, neboť nevychází z podstatných peněžních toků, nýbrž z účetních veličin a je tak opomíjena například změna čistého pracovního kapitálu.

U kritérií, která vycházejí z finančních toků, jsou efekty vyjádřeny užitím příjmů a výdajů v jednotlivých fázích projektu. Finanční toky jsou nejčastěji vyjádřeny jako rozdíl provozních příjmů a kapitálových výdajů a jejich obsah závisí na typu kritéria a způsobu financování projektu. Rozlišovány jsou například volné finanční toky *FCF*, finanční toky z aktiv *FCFF* a finanční toky z vlastního kapitálu *FCFE*. Velkou výhodou těchto kritérií je zaměření na skutečné a nezkreslené efekty, jež jsou projektem generovány. Výpočet je nicméně relativně obtížnější oproti kritériím účetním.

3.2.4 **Paramtery hodnocení investic**

Dluhošová (2010) uvádí jako základní parametry hodnocení investic, na kterých jsou založeny metody kvantifikování ziskovosti a efektivnosti projektů, jež jsou popsány v podpodkapitole 3.2.5, relevantní peněžní toky FCF, náklad kapitálu R, čistou současnou hodnotu NPV a dobu životnosti investice T.

Stanovení ***peněžních toků*** investice je klíčové pro korektní vyhodnocení efektivnosti investičního projektu. Volné peněžní toky v rámci investice FCF tvoří příjmy a výdaje, jež jsou generovány v souvislosti s investičním projektem. V případě podnikové sféry, kdy podnik po dobu před investičním projektem generuje příjmy, jsou volné peněžní toky investice určeny na principu změnového přírůstku. Jedná se o ty příjmy a výdaje, které jsou změnou oproti situaci před realizací projektu. Pro tzv. investiční projekty na zelené louce jsou všechny příjmy a výdaje součástí volných peněžních toků FCF. Peněžní toky jsou tvořeny dvěma základními složkami: jednorázové kapitálové výdaje a provozní příjmy v době provozování investice.

Jednorázové kapitálové výdaje tvoří výdaje na pořízení dlouhodobého hmotného nebo nehmotného majetku INV a výdaje na kladnou změnu čistého pracovního kapitálu $\Delta\,ČPK$. Vztah pro výpočet kapitálových výdajů lze napsat takto:

$$JKV = INV + \Delta\,ČPK \tag{3.19}$$

Jestliže se neuvažuje dodatečné investování v průběhu provozu projektu, pak jsou budoucí očekávané příjmy z investice (FCF) tvořeny čistým ziskem (EAT), odpisy (ODP) a odpočtem změny $ČPK$. Pro nezadluženou investici tak platí:

$$FCF = EAT + ODP - \Delta\,ČPK \tag{3.20}$$

Definování ***nákladů na kapitál*** je klíčovou součástí při hodnocení efektivnosti projektů založených na kritériích s využitím faktoru času, neboť je náklad kapitálu užíván jako diskontní sazba pro výpočet čisté současné hodnoty projektu. Velikost nákladu na kapitál je ovlivněna mnoha faktory, například způsobem financování nebo rizikovostí projektu. Ke stanovení nákladu na kapitál se využívá několik přístupů.

Náklady podniku na získávání podnikového kapitálu se nazývají náklady kapitálu a představují minimální požadovanou výnosnost kapitálu. Tyto náklady je možné chápat

z pohledu investora a z pohledu podniku. Z pohledu investora se jedná o požadavek na výnosnost dosahovanou podnikem, aniž by došlo k poklesu bohatství pro investora. Z pohledu podniku jde o cenu za kapitál, který je potřebný k dalšímu rozvoji činnosti společnosti.

Velikost nákladu na kapitál je obecně závislá na rizikovosti jednotlivých aktiv. Je možné zapsat velikost nákladu na kapitál jako součet bezrizikové míry a rizikové prémie, jež je odlišná pro různé druhy finančních instrumentů. Riziková prémie kompenzuje investorovi vyšší nejistotu ohledně budoucího výnosu aktiva.

V souvislosti se způsobem financování se rozlišují různé druhy nákladu na kapitál. Jsou jimi náklady na cizí, vlastní a celkový kapitál. Náklady na celkový kapitál, nebo též vážené průměrné náklady kapitálu (WACC), tvoří náklady různých forem kapitálu, vlastní a cizí. Vzorec pro výpočet je následující:

$$WACC = \frac{R_E \cdot E + R_D \cdot (1-t) \cdot D}{E + D}, \tag{3.21}$$

kde R_E odpovídá nákladům na vlastní kapitál, E značí vlastní kapitál, R_D jsou náklady úročeného cizího kapitálu, D je úročený cizí kapitál a t je sazba příjmové daně.

Náklady kapitálu jsou tvořeny dvěma složkami, vlastním a cizím kapitálem. Podíl těchto dvou složek na celkovém kapitálu je vždy potřeba vyčíslit na základě tržních hodnot, nikoliv účetních, neboť by mohlo být porušeno pravidlo vnitřní konzistence tržního odhadu. Protože ne vždy je možné tržní data získat, použití účetních dat je v tomto případě nutno chápat jen jakousi aproximaci tržních podmínek.

Náklady na cizí kapitál lze definovat jako kuponové nebo úrokové platby placené věřitelům za možnost využití kapitálu. Výše kuponových a úrokových plateb je dána jednak základní úrokovou mírou na trhu, a jednak závisí na několika dalších faktorech. Těmito faktory je čas, bonita dlužníka a očekávaná efektivnost z nakládání s půjčenými penězi. Z hlediska času platí přímá úměra, neboť s rostoucí délkou období, na které je úvěr poskytnut, roste i cena úvěru. U zbylých dvou faktorů se jedná o úměru nepřímou, neboť vyšší bonita dlužníka a očekávaná efektivnost, v konečném důsledku snižují cenu cizího kapitálu.

Náklady na cizí kapitál jsou obecně nižší než náklady na kapitál vlastní. Jedním z důvodů je vyšší riziko vkladu pro vlastníka, neboť vkládá své prostředky na teoreticky neomezenou dobu, přičemž nemá zaručen jakýkoliv výnos z tohoto vkladu. Věřitel má naproti

tomu zaručen pravidelný výnos a peníze vkládá na přesně vymezenou dobu. Dalším důvodem je charakter úrokových nákladů, jež jsou daňově uznatelné a snižují zisk jako základ pro výpočet daňové povinnosti. Na základě této logiky jsou náklady kapitálu, který firma získá formou dluhu R_D, vyjádřeny následovně:

$$R_D = i \cdot (1 - t), \tag{3.22}$$

kde i je výše úrokové míry dluhu a t značí sazbu daně.

Získá-li podnik kapitál upisováním obligací, náklad dluhu se určí jako výnos do splatnosti obligace:

$$P = \sum_{t=1}^{T} c_t \cdot (1 + R_D)^{-t} + NV \cdot (1 + R_D)^{-T}, \tag{3.23}$$

kde c vyjadřuje kuponovou platbu, NV je nominální hodnota obligace, T značí dobu do splatnosti obligace a P je tržní cena obligace.

Náklady na *vlastní kapitál* je možné určit na bázi tržních, ale i účetních přístupů a metod. Výběr metody závisí zejména na dostupnosti dat, což souvisí s vyspělostí finančních trhů a tržními podmínkami. K určení nákladů na vlastní kapitál se využívají tyto metody:

- model oceňování kapitálových aktiv (CAPM),
- arbitrážní model oceňování (APM),
- dividendový růstový model,
- stavebnicové modely.

Detailnější popis bude věnován pouze modelu CAPM, neboť je využit k výpočtu diskontní sazby pro stanovení čisté současné hodnoty. Pro ostatní metody platí, že jsou alternativami k výpočtu nákladu na vlastní kapitál. V případě APM a dividendového růstového modelu se jedná o metody využívající tržních dat a jejich využití, stejně jako využití CAPM, je možné pouze tam, kde jsou data pro výpočet dostupná. Stavebnicové modely se využívají v ekonomice s nedokonalým kapitálovým trhem a data pro výpočet pocházejí z účetních dat podniků. Princip stavebnicových modelů spočívá v kvantifikaci rizikových přirážek za konkrétní druh rizika a jejich připočítání k bezrizikové výnosnosti.

Model oceňování kapitálových aktiv je tržním přístupem pro stanovení nákladů na vlastní kapitál. Ve světové praxi se jedná o důležitý model k určení diskontní sazby pro tržní

ocenění. Jde o rovnovážný model oceňování kapitálových aktiv, kde rovnováha je dána rovností mezního sklonu očekávaného výnosu a rizika pro všechny investory. Metoda CAPM je založena na funkčním lineárním vztahu mezi výnosem konkrétního aktiva a tržního portfolia, které definuje riziko celého trhu. Jedná se o jednofaktorový model. Beta verze modelu CAPM – SML je následující:

$$E(R_E) = R_F + \beta_E \cdot [E(R_M) - R_F], \tag{3.24}$$

kde $E(R_E)$ je očekávaný výnos vlastního kapitálu, R_F reprezentuje bezrizikovou sazbu, $E(R_M)$ značí výnos tržního portfolia a β_E je koeficient citlivosti dodatečného výnosu kapitálu na dodatečný výnos trhu.

Koeficient β_E lze vypočítat pomocí tohoto vzorce:

$$\beta_E = \frac{\text{cov}(R_E; R_M)}{\text{var}(R_M)}, \tag{3.25}$$

kde $\text{cov}(R_E; R_M)$ je kovariance výnosů aktiva a tržního portfolia a $\text{var}(R_M)$ je rozptyl výnosů tržního portfolia.

Doba životnosti projektu představuje dobu pro kterou se provádí odhad budoucích peněnžích toků. Důležité je rozlišovat mezi technickou a ekonomickou životností projektu. Technická životnost se odvíjí od fyzického opotřebení zařízení investice a je definována technickými parametry majetku. Naproti tomu ekonomická životnost je ovlivněna ekonomickou využitelností produktů projektu, technickým pokrokem nebo zdroji surovin. Z logiky věci vyplývá, že ekonomická životnost nemůže být delší než životnost technická.

3.2.5 **Kritéria hodnocení nezadlužených investic**

Mezi kritéria hodnocení nezadlužených investic dle Dluhošové (2010) patří čistá současná hodnota, index ziskovosti, vnitřní výnosové procento, doba úhrady a rentabilita investovaného kapitálu.

Kritérium ***čisté současné hodnoty*** je založeno na výpočtu rozdílu mezi současnou hodnotou všech bucoucích příjmů z investice a současné hodnoty výdajů na investiční projekt. Z názvu čistá současná hodnota je patrné, že se jedná o přebytek mezi diskontovanými příjmy a výdaji, který lze interpretovat jako absolutní přírůstek majetku podniku z realizace projektu. Pro projekt s kladnou NPV tedy platí, že v konečném důsledku zvyšuje hodnotu podniku,

protože očekávaná výsnosnost je vyšší než náklady na kapitál. Naopak projekt se zápornou *NPV* snižuje podnikovou hodnotu. Realizován tedy bude takový projekt jehož $NPV > 0$ a naopak nebude realizován projekt s $NPV < 0$. V případě, kdy je *NPV* rovno nule, je pouze na rozhodujících subjektech, zdali dojde k realizaci projektu. Výpočet *NPV* lze zapsat takto:

$$NPV = \sum_{t=1}^{T} FCF_t (1+R)^{-t} - JKV \,, \tag{3.26}$$

kde *R* je náklad na kapitál, *T* značí dobu životnosti projektu, *JKV* jsou počáteční kapitálové výdaje a FCF_t jsou volné peněžní toky v době investice.

Výhodou daného kritéria je zejména respektování faktoru času, možná změny nákladu kapitálu v čase a aditivita. Aditivita znamená možnost sčítání *NPV* jednotlivých projektů a platí následující vztah:

$$NPV_p = \sum_i NPV_i \,. \tag{3.27}$$

Nevýhodou je možnost úmělého nadhodnocení NPV projektu zvýšením doby životnosti, která neodpovídá reálným podmínkám.

IRR neboli ***vnitřní výnosové procento*** vyjadřuje velikost roční průměrné diskontní sazby, při které je rozdíl mezi současnou hodnotou provozních peněžních toku a kapitálovými výdaji rovna nule. Rovnici pro výpočet vnitřního výnosového procenta lze napsat takto:

$$\sum_{t=1}^{T} FCF_t (1+IRR)^{-t} = JKV \,. \tag{3.28}$$

V případě nekonvenčních finančních toků může mít výpočet *IRR* více reálných řešení. Výsledek je možné získat na základě využití iteračního přibližovacího algoritmu, přičemž velmi jednoduchým způsobem využití funkce IRR v Excelu. Parametry funkce jsou finanční toky investice (s minusovou hodnotou jednorázových kapitálových výdajů) a odhad, který slouží jako výchozí hodnota *IRR* pro iterační výpočet.

Dle kritéria založeného na vnitřním výnosovém procentu by podnik měl realizovat investiční, projekt pokud je vnitřní výnosové procento vyšší než náklad na kapitál s obdobným rizikem. Čím více vnitřní výnosové procento převyšuje náklad kapitálu srovnatelného rizikového projektu, tím je projekt ekonomicky výhodnější.

Mezi výhody tohoto kritéria lze zařadit výpočet na základě finančních toků a respektování faktoru času. Naopak nevýhodou může být nadhodnocení projektu prodlužováním doby životnosti nebo možný vznik více řešení.

Doba úhrady značí časový interval, za nějž kumulované provozní příjmy od začátku projektu vyrovnají počáteční kapitálové výdaje na investiční projekt. Rozlišují se dvě verze doby úhrady, a to diskontovaná a statická, přičemž rozdílem je diskontování provozních příjmů z investice. Ve své podstatě se jedná o nalezení takové doby úhrady ($DÚ$), pro niž platí:

$$\sum_{t=1}^{DÚ} FCF_t (1+R)^{-t} = JKV. \tag{3.29}$$

Je-li doba úhrady kratší než limitně určená doba u daných typů projektů, projekt by měl být přijat. Kritérium je vhodné pro hodnocení krátkodobých investičních projekt, kde je požadována rychlá návratnost vložených prostředků. Jistou nevýhodou je, že nejsou brány v potaz finanční toky po době úhrady projektu a nemožnost sčítání projektů.

4 Posouzení ziskovosti těžby

Čtvrtá kapitola je stěžejní kapitolou celé práce, neboť je zaměřena na výpočet ziskovosti investice do těžebních zařízení. Úvodem kapitoly jsou popsány vstupní a průběžné výdaje a podstatné informace s nimi související, jež je potřeba zvážit před samotnou investicí. Kapitola pokračuje popisem a posouzením ziskovosti jednotlivých variant. Nejprve jsou pro každou variantu popsány provedené simulace zaměřené na predikci ceny bitcoinu a celkového výpočetního výkonu bitcoinové sítě. A poté je pro každou variantu posouzena ziskovost těžby bitcoinu za využití metody čisté současné hodnoty. Kapitola je zakončena shrnutím výsledků.

4.1 Vstupní a průběžné výdaje

Tato podkapitola je věnována popisu vstupních a průběžných výdajů v jednotlivých letech investice. Nejprve jsou popsány počáteční výdaje na těžící zařízení a věci s tímto související. Následná část souvisí s popisem průběžných výdajů na elektřinu, jež jsou také největšími výdaji po celou dobu investice. Podkapitola je zakončena rozborem finančních veličin vstupujících do samotného výpočtu konečné ziskovosti těžby.

Nákup ***hardware*** je největším počátečním výdajem, který je potřeba vynaložit, aby těžba mohla vůbec začít. Velikost tohoto počátečního výdaje závisí jednak na výběru těžícího přístroje, a jednak na množství těchto strojů, které k těžbě budou využity. V reálné situaci je počáteční výdaj ovlivněn disponibilními prostředky těžaře. V rámci práce není výše počátečního výdaje nijak ovlivněna a druh přístroje a množství je možné zvolit zcela individuálně.

Na trhu je k 2. 2. 2018 ke koupi a využívání velké množství těžících přístrojů. Nicméně jako je tomu u aut, počítačů nebo mobilů, je možné vždy najít věc, která překoná ostatní možnosti v poměru cena a výkon. V případě těžících přístrojů je tomu obdobně a z množství různých variant je po kompletní analýze možné vybrat ten momentálně nejlepší. Výběr nejlepšího těžícího přístroje závisí zejména na množství peněžních prostředků, které je nutno vynaložit na koupi samotného přístroje, ale také na penězích vynaložených za elektřinu v průběhu těžby, přičemž nejlepší přístroje se vyznačují nejnižší spotřebou elektřiny na jeden GH/s.

Na základě odborných recenzí a článků je v práci počítáno s využitím přístroje s názvem Antminer S9. Důvodem jsou následující skutečnosti:

- Nejvyšší výpočetní výkon na jeden přístroj ve velikosti 13,5 TH/s.[7] U některých zařízení S9 je uváděn výpočetní výkon ve velikost 14 TH/s nebo také 12.93 TH/s. V práci je počítáno s výkonem 13,5 TH/s. Je potřeba zmínit, že na trh bude v dubnu roku 2018 uveden těžící přístroj s názvem Dragonmint 16T, jehož výpočetní výkon dosahuje až 16 TH/s. Protože je nutné zakoupit minimálně 5 kusů a dnešním dnem (1. 2. 2018) je možné daný přístroj pouze předobjednat, nebude brán jako relevantní konkurent přístroji Antminer S9.
- Antminer S9 je nejefektivnější těžící zařízení[8] na trhu spolu s přístrojem Antminer R4 – 0,098 J/GH/s. Jelikož má Antminer S9 větší výpočetní výkon bude vybrán tento.
- Z hlediska ceny je Antminer S9 dražší, než ostatní těžící přístroje. Cena za jeden přístroj činí 2000 USD, viz. obr. 4-1 a s touto cenou je dále počítáno. Vzhledem k vysoké efektivnosti a velkému výpočetnímu výkonu je tato cena odůvodnitelná. Je potřeba také zmínit, že cena zařízení se výrazně liší od prodejce a měsíce ve kterém je prodáván. Obr. 4-1 shrnuje zhodocení vybraného těžícího zařízení.

Obr. 4-1: Antminer S9

Zdroj: www.99bitcoins.com

K zařízení je nutno zakoupit také zdroj, který odpovídá celkovému příkonu přístroje. Cena zdroje se pohybuje okolo 200 USD[9], činí tedy přibližných 10 % z ceny. Celkové výdaje

[7] Odkaz:https://bitcointalk.org/index.php?topic=2676763.0
[8] Odkaz:https://www.techradar.com/news/best-asic-devices-for-bitcoin-mining-in-2018
[9] Odkaz: https://www.banggood.com/2800W-One-Way-Mining-Miner-Mining-Rig-Power-Supply-Antminer-246P-S7-S9-L3-L3-p-1210997.html?rmmds=detail-left-hotproducts__3&cur_warehouse=CN

na dva těžící přístoje s dvěmi zdroji činí 88 717 CZK (přepočet dle kurzu k 2. 2. 2018). Kumulativní výpočetní výkon těchto dvou přístrojů dosahuje 27 000 GH/s.

V této práci budeme dále vycházet z následujících předpokladů:

Těžař žije v bytě sám, přičemž celková spotřeba je průměrná (na osobu dle dat českého statistického úřadu se jedná o 1 335kWh za rok[10]) a vybavení domácnosti standardní. Z toho vyplývá, že jako potřebný a velmi dostačující jistič v bytě lze brát jistič 3x10 A – 3x16 A. Vzhledem k tomu, že do této domácnosti přibudou dva těžební přístroje s příkonem 1323 wattů na jeden, bude potřeba změnit typ jističe. Změna jističe zvýší průběžné měsíční výdaje a v rámci celkového výpočtu bude počítáno se změnou výdajů v důsledku navýšení jističe, nikoli celý měsíční výdaj za jistič. Původní jistič 3x10 A – 3x16 A bude změněn na jistič 3x20 A – 3x25 A. Výši nutné změny jističe lze vypočítat pomocí vzorce $P = U \cdot I$ (kde P vyjadřuje výkon, U napětí a I označuje proud). Transformací pro výpočet proudu dostáváme rovnici $I = \frac{P}{U}$, přičemž dosazením do vzorce lze vypočíst změnu proudu po přidání těžících přístrojů. Tedy $I = \frac{1323 * 2}{240} = 11{,}025\,\text{A}$. Pokud by došlo k navýšení počtu těžících zařízení, bylo by nutno jistič opět měnit, což by v konečném důsledku opět znamenalo navýšení měsíčního poplatku energetické společnosti.

Protože připojením těžebních zařízení razantně vzroste spotřeba, bude počítáno s distribuční sazbou D02d, což je standardní sazba pro domácnosti se střední nebo vyšší spotřebou. Celkový měsíční výdaj za elektřinu bude počítán následovně dle sazebníku společnosti ČEZ s fixací ceny na 3 roky. Platba elektřiny za měsíc v závislosti na velikost spotřeby je zobrazena v tabulce 4-1.

Tabulka 4-1: Výpočet spotřeby elektřiny

Řádek	Druhy plateb	Kč
1	Stálá platba/měsíc	72.6
2	Doplatek za jistič/měsíc	39.93
3	Činnost OTE/měsíc	6.53
4	Celková jednotková cena/Mwh	3 316.39
5	Poplatek na podporu výkupu elektřiny z obnovitelných zdrojů/Mwh	598.95
6	Celkem za elektřinu/Mwh - řádek 4 + 5	3 915.34
7	Měsíční platby celkem - řádek 1 + 2 + 3	119.06

Zdroj: www.cez.cz

[10]https://www.czso.cz/csu/xs/spotreba-paliv-a-energii-v-domacnostech-stredoceskeho-kraje

Vzhledem k příkonu dvou těžících přístojů ve velikost 2 646 wattů činí měsíční spotřeba při stálém provozu 1,905 megawatthodin. Celková měsíční platba za elektřinu je rovna 7 578 Kč. Výpočet měsíční spotřeby je následujcící:

$$Celková\ spotreba\ (MWh) = \frac{24 \cdot 30 \cdot 2\,646}{1\,000\,000},$$

kde 24 je denní počet hodin, 30 značí počet dní v měsíci, 2 646 (wattů) je příkon těžícího zařízení a 1 000 000 je koeficient pro přepočet na megawatthodiny.

Další důležité vstupní údaje a předpoklady (k 2. 2. 2018) jsou:

- aktuální odměna za nalezení bloku je 12.5 BTC,
- doba trvání projektu činí 3 roky a veškeré požadované míry výnosnosti (diskontní sazby) jsou stanoveny jako roční, neboť NPV je počítána na roční bázi. Veškeré vytěžené bitcoiny za konkrétní rok jsou prodány vždy na konci daného roku za aktuální cenu, což je celkový výnos těžaře za jeden rok,
- poplatek poolu je roven 2 %,
- jsou uvažovány daně a odpisy těžícího zařízení,
- nejsou uvažovány náklady na provoz internetu a chlazení,
- pro přepočet USD na CZK je brán kurz 20.163 (2. 2. 2018)[11],
- je předpokládána perfektní korelace mezi vývojem ceny a hash rate,
- simulace je provedena na bázi geometrického Brownova pohybu měsíčně- 36 kroků.

Na základě vyjádření mluvčí Generálního finančního ředitelství Petry Petlachové[12] je uvažována výše daně v hodnotě 15 %, neboť prodej bitcoinů může být u fyzické osoby předmětem daně jako příjem podle § 7 zákona o daních z příjmů. Od příjmů se odečnou všechny výdaje vynaložené v souladu se ZDP na dosažení, zajištění a udržení těchto příjmů. Dále je uvažováno s možnostní uplatnění daňové ztráty z těžby bitcoinů jako položky snižující základ daně dle § 34 ZDP.

Dlouhodobý majetek je z hlediska daňových odpisů rozdělen do šesti odpisových skupin, které se liší dobou odepisování. Pro těžící zařízení platí, že je zařazeno do odpisové skupiny první, kde doba odepisování činí 3 roky. Do první odpisové skupiny patří těžící zařízení, neboť je možné jej zařadit do položky (1 -15) – počítače a periferní zařízení.

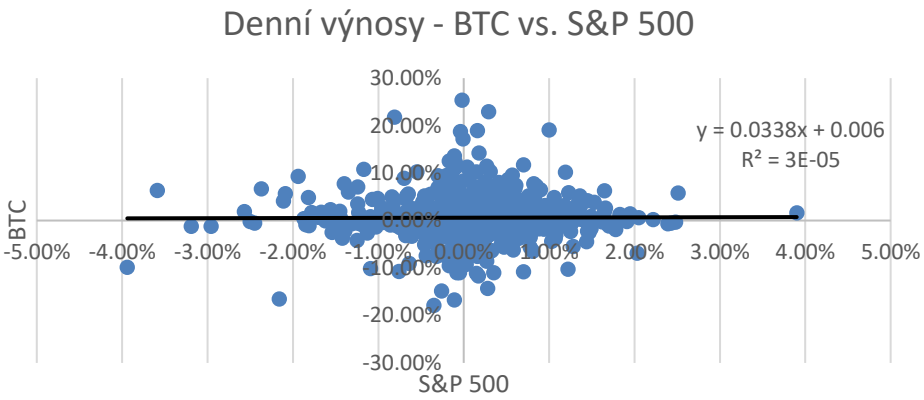
[11] Odkaz: https://www.kurzy.cz/kurzy-men/historie/USD-americky-dolar/
[12] Odkaz: https://www.mesec.cz/clanky/jak-se-dani-virtualni-meny-cast-zisku-odvedete-vzdy-bitcoin-je-pro-bernak-vec/

Odepisování bude probíhat rovnoměrně a daňové odpisy se rovnají účetním. Odpisy v první roce činí 20 % z pořizovací ceny a 40 % v následujících letech. Počátek projektu je datován ke dni 2. 2. 2018. Konec projektu k datu 2. 2. 2021.

4.1.1 Stanovení diskontní míry

Pro výpočet čisté současné hodnoty je potřeba určit výšši požadované výnosnosti projektu, jež slouží v samotném výpočtu jako diskontní míra. Požadovanou míru výnosnosti lze stanovit mnohými způsoby. Jednou z možností, jak stanovit požadovanou výnnosnost, je využití modelu CAPM. Vzhledem k dostupnosti dat a relativně snadnému výpočtu, je využití daného modelu naprosto příhodné. Klíčová pro výpočet míry výnostnosti je znalost beta koeficientu aktiva, pro něhož je požadovaná výnosnost počítána, v tomto případě pro bitcoin. Ke kvantifikování koeficientu beta je využíván vzorec (3.25), kde v čitateli je kovariance mezi výnosností aktiva a výnosností trzního indexu a ve jmenovateli rozptyl výnosů tržního indexu. Jako tržní index je vybrán index S&P 500 a je počítáno s denními a měsíčními daty[13].

Graf 4-1: Závislost denních výnosů bitcoinu a indexu S&P 500



Zdroj: vlastní zpracování

V případě denních (1. 2. 2015 – 1. 2. 2018) výnosů bitcoinu a indexu S&P 500 vychází kovariance 0,000002, což naznačuje, že se hodnoty neovlivňují, tedy jsou nezávislé. Beta koeficient vychází 0,035, což potvrzuje nezávislost mezi denními výnosy bitcoinu[14] a indexem S&P 500. Jestliže by byla požadovaná míra výnosnosti počítána s využitím tohoto beta koeficientu, její výše by dosahovala přibližně hodnot výnosu bezrizikového aktiva. Vzhledem k podstupovanému riziku je taková diskontní míra velmi nizká a nebude proto dále uvažována. Protože je závislost téměř nulová, bitcoin lze vnimat jako zajímavý nástroj pro diverzifikaci

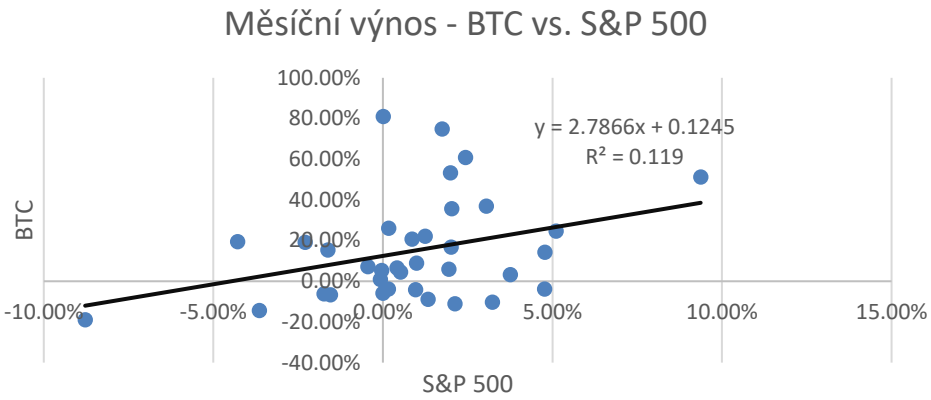
[13] Odkaz: https://fred.stlouisfed.org/series/SP500
[14] Odkaz: https://www.coindesk.com/price/

portfolia finančních aktiv. Vzhledem k vysoké volatilitě ovšem není příhodné investovat velkou procentní část finančních prostředků do bitcoinu.

Kovariance s využitím měsíčních výnosů (1. 2. 2015 – 1. 2. 2018) je rovna hodnotě 0.002583 a rozptyl tržního portfolia reprezentovaného indexem S&P 500 činí 0.000927. Dosazením do vzorce (3.25) pro výpočet beta koeficientu bitcoinu vychází beta 2.78. Využitím modelu CAPM dle vzorce (3.24) vychází náklady na vlastní kapitál 16,70 %, přičemž hodnoty dosazené do vzorce spolu s koeficientem beta jsou tyto:

- bezriziková sazba = 2.58 % (výnos 10-letých amerických dluhopisů k počátku roku 2018[15]),
- riziková prémie (země Spojené státy americké) 5,08%[16].

Graf 4-2: Závislost měsíčních výnosů bitcoinu na S&P 500



Zdroj: vlastní zpracování

Jelikož je hodnota požadované míry výnosnosti závislá na subjektu investující finanční prostředky do projektu a v mnoha případěch se může značně lišit, bude k výpočtu čisté současné hodnoty, spolu s mírou výnosnosti dle modelu CAPM, využito množiny požadovaných měr výnosností (10 %, 20 %, 30%, 40 %, 50 %, 60 %).

4.2 Posouzení ziskovosti

Projekty s kladnou čistou současnou hodnotou by měly být realizovány, neboť v konečném důsledku zvyšují hodnotu majetku podniku. Naopak projekty se zápornou čistou současnou hodnotou je logické neprovádět a hledat jiné alternativy. V této části práce jsou demonstrovány výsledky zvolených variant projektu. Ke konečnému posouzení ziskovosti

[15] Odkaz: http://www.multpl.com/10-year-treasury-rate/table/by-year
[16] Odkaz: http://pages.stern.nyu.edu/~adamodar/

těžby je využito 3 variant vývoje ceny bitcoinu a hash rate, přičemž pro každou variantu je vytvořeno 10 000 různých scénářů vývoje. První varianta je základní a odráží historický vývoj ceny bitcoinu a hash rate v letech 2015 – 2018. Druhá varianta vychází z predikce cen významného obchodníka ve světě kryptoměn, přičemž se jedná o značně optimistickou predikci. Poslední varianta je jediná pesimistická a je zde předpoklad postupného snižování ceny bitcoinu po dobu investice. Z počátku každé varianty je nejprve popsán simulovaný vývoj ceny bitcoinu a hash rate. S využitím těchto dat je posléze posouzena ziskovost těžby za pomocí metody čisté současné hodnoty. Část zaměřená na čistou současnou hodnotu je strukturována tak, že je nejprve popsán počet vytěžených bitcoinů za dobu projektu, následně je popsáno rozdělení pravděpodobnosti čisté současné hodnoty a na konec jsou prezentovány výsledky možnosti, kdy těžař nekupuje a netěží s dvěmi těžícími zařízeními, nýbrž pouze s jedním. Detailní data rozdělení pravděpodobnosti čisté současné hodnoty jsou uvedeny v příloze.

V grafech popisujících simulaci ceny bitcoinu a hash rate jsou vyobrazeny intervaly spolehlivosti, tedy intervaly do kterých bude spadat cena na konci vybraného období v rámci konkrétní pravděpodobnosti. Tyto grafy budou využity pro popis vývoje ceny a celkového hash rate v případě všech tří variant. Ke grafům bude v příloze uvedená datová tabulka, aby měl čtenář plný vhled na hraniční hodnoty intervalů po celé období. V popisu je upřednostněno zejména poslední období v každém roce. Jako výchozí data pro výpočet střední hodnoty a směrodatné odchylky ceny bitcoinu[17] a hash rate[18] jsou brána data z prvního dne každého měsíce v období, z kterého vychází konktrétní varianta.

4.2.1 Varianta vycházející z historické časové řady

První varianta je mírně optimistickou, nikoliv však pesimistickou, odráží vývoj v posledních třech letech. Výpočet střední hodnoty a směrodatné odchylky je založen na měsíčních datech v období od 1. 2. 2015 – 1. 2. 2018. Simulace ceny bitcoinu a hash rate prvního scénáře je počítána s následujícími hodnotami:

Tabulka 4-2: Vstupní údaje pro první variantu

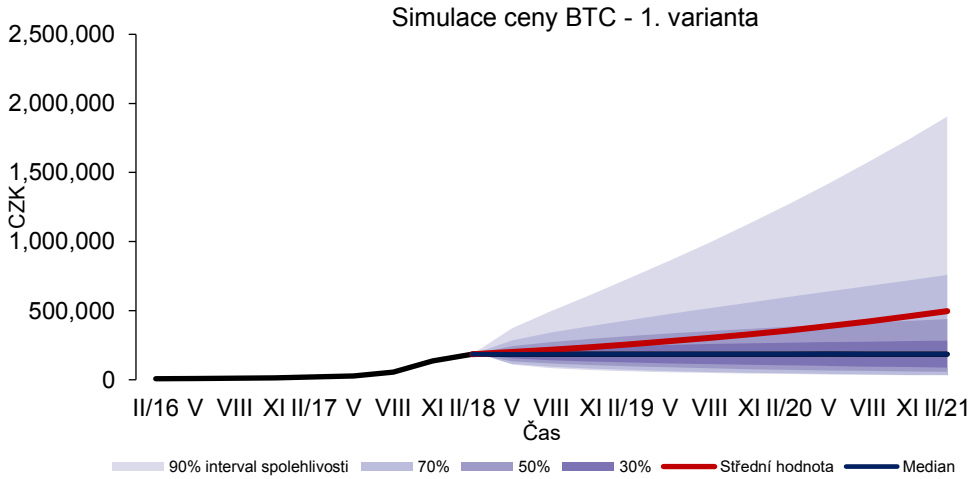
	Hash rate	Cena
Střední hodnota	41.77 %	32.95 %
Směrod. odchylka	32.84 %	87.36 %
Interval	0.083333	0.083333
Výchozí hodnota	2.07E+10 GH/s	184 905 CZK

Zdroj: vlastní zpracování

[17] Odkaz data: https://www.coindesk.com/price/
[18] Odkaz data: https://data.bitcoinity.org/bitcoin/hashrate/all?c=m&g=15&t=a

Z prvního grafu 4-3 je patrné, že dochází k postupnému rozšiřování rozpětí ceny pro vybrané intervaly spolehlivosti, což pokračuje po celé sledované období. Pokles spodní hranice intervalů je ovšem mnohem pozvolnější, než nárůst horní hranice, a signifikuje rostoucí střední hodnotu. Střední hodnota se v období 2018 – 2021 postupně zvyšuje a z počátečních 184 905 CZK činí 496 841 CZK k únoru roku 2021. Z grafu 4-3 je také patrné, že jsou simulované ceny bitcoinu log-normálně rozděleny, což znamená nesymterické rozdělení s kladnými hodnotami. Rozdělení simulované ceny je kladně zesiškmeno, neboť hodnoty vyšší než průměr jsou od průměru odlehlejší oproti hodnotám nižším než průměr. Například v rámci 90% intervalu spolehlivost je maximální očekávaná cena bitcoinu k 2. 2. 2021 rovna 1 905 241 CZK a minimální 13 127 CZK. Medián se výrazně nemění, neboť oproti střední hodnotě není ovlivněn extrémními hodnotami. Na konci simulovaného období je ve výši 185 793 CZK.

Graf 4-3: Simulace ceny bitcoinu - 1. varianta

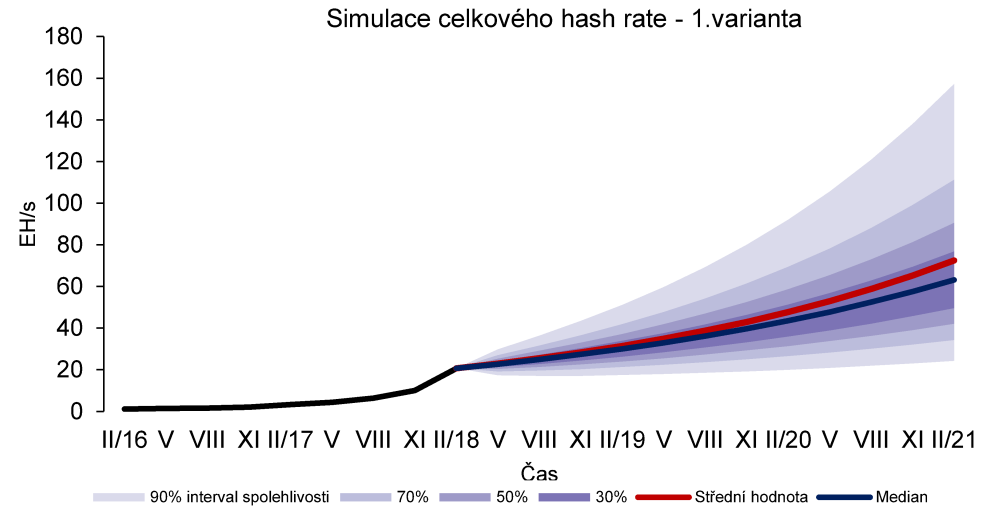


Zdroj: vlastní zpracování

Pro vývoj celkového hash rate platí podobné závěry, jako u vývoje ceny, tedy pozvolné rozšiřování jednotlivých intervalů a rostoucí střední hodnota, viz graf 4-4. Celková změna střední hodnoty během období investice činí 52 EH/s, tedy přibližne 17.3 EH/s za jeden rok. Medián se s časem zvyšuje a k 1. 2. 2021 dosahuje hodnoty 63.1 EH/s. Jelikož není medián ovlivněn extrémními hodnotami, je zřejmé, že u velkého počtu scénářů dochází k růstu hash rate. Simulované hodnoty hash rate mají log-normální rozdělení a toto rozdělení je kladně zešikmeno. S 90% pravděpodobnosti může konečná hodnota hash rate, tedy k datu 2. 2. 2021, činit až 157.16 EH/s. Dolní hranice intervalu je rovna 24.19 EH/s, což je stále vyšší hodnota, než výchozí. V reálném světě by takováto výpočetní síla znamenala obrovskou spotřebu energie, téměř nereálnou na dnešní kapacity. Jelikož však lidé neustále zefektivňují různé přístroje a snižují jejich energetickou náročnost, je teoreticky možné, že by nárůst výpočetního

výkonu nezpůsobil energetickou a ekologickou katastrofu, která by se současnými přístroji, při takovémto vývoji hashrate, možná nastala.

Graf 4-4: Simulace hashrate - 1. varianta

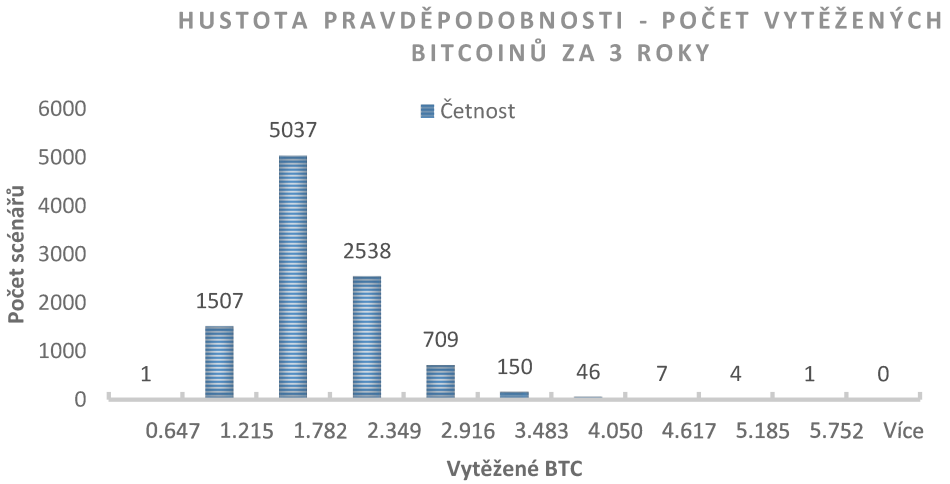


Zdroj: vlastní zpracování

Čistá současná hodnota – 1. varianta

Jak bylo zmíněno v první kapitole, je množství vytěžených bitcoinů závislé na dvou parametrech. Jednak záleží na výpočetní síle náležející těžaři, a jednak jde o výpočetní výkon celkový. Vzhledem k výpočetnímu výkonu v řádech desítek EH/s jsou počty vytěžených bitcoinů jednotlivcem absolutně nízké.

Graf 4-5: Celkový počet vytěžených bitcoinů - 1. varianta



Zdroj: vlastní zpracování

Tato skutečnost je patrná také z grafu 4-5, který je zaměřen na shrnutí kumulativního počtu vytěžených bitcoinů v průběhu celé investice. Ve více než polovině scénářu dosahuje počet vytěžených bitcoinů za tři roky hodnot mezi 1.215 - 1.728. Relativně velký počet scénářů spadá do intervalů sousedních, přičemž více než u čtvrtiny z celkových scénářů, je to interval od 1.782 do 2.349 vytěžených bitcoinů. Počet scénářů pro vyšší rozmezí postupně klesá až k hranici 5.752, což je maximální počet vytěžených bitcoinů a je ho dosaženo pouze v jednom z desíti tisíc scénářů.

Množství vytěžených bitcoinů je důležitým indikátorem pro posouzení ziskovosti těžby, nicméně až v kombinaci s cenou, za kterou je možné tyto bitcoiny prodat, a náklady na těžbu, je získána podstatná informace o efektivnosti těžby. Využitím parametru čisté současné hodnoty je kvanitifkován přínos těžby v podobě růstu hodnoty pro těžaře. V tabulce 4-3 jsou zobrazeny počty scénářů, pro které platí, že je výsledná hodnota NPV záporná a počty scénářů s opačnou podmínkou. Přestože se nejedná o pesimistickou variantu, více než u 2/3 všech scénářů vychází NPV záporná.

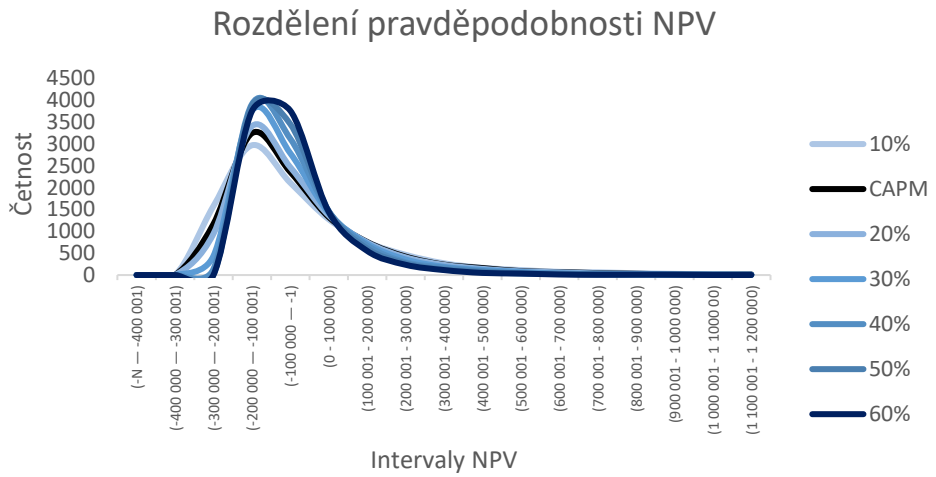
Tabulka 4-3: Poměr kladných a záporných NPV – 1. varianta

Míry výnosnosti	10 %	CAPM	20 %	30 %	40 %	50 %	60 %
NPV < 0	6 667	6 778	6 824	6 992	7 173	7 349	7 519
NPV > 0	3 333	3 222	3 176	3 008	2 827	2 651	2 481

Zdroj: vlastní zpracování

Graf 4-6 vyobrazuje počty scénářů v různých variantách požadované míry výnosnosti, pro které platí, že jejich čistá současná hodnota se nachází v jedné z mezí uvedené v dolní části grafu. Z grafu 4-6 je zřejmé, že pro větší počet scénářů vychází NPV záporná a pro absolutně nejvíc scénářů všech požadovaných měr výnosnosti se výsledné NPV nachází v intervalu od -200 000 CZK do -100 001 CZK. Pro scénáře s kladnou NPV platí, že ve většině případů bude výsledná NPV od 0 do 100 000 CZK. Rozdělení je kladně zešikmeno, neboť u malého procenta scénářů vychází hodnota NPV vyšší, než je maximální možná ztráta z projektu.

Graf 4-6: Rozdělení pravděpodobnosti NPV - 1. varianta



Zdroj: vlastní zpracování

Pro zvýšení vypovídací schopnosti grafu 4-6 je přiložena tabulka 4-4. V této tabulce jsou vypsány důležité hodnoty NPV pro každou velikost požadované míry výnosnosti. Průměr NPV je informací, která dokládá, že i s předpokladem růstu ceny bitcoinu není zajištěna ziskovost celého projektu. Mohou nastat situace, kdy je cena bitcoinu natolik vysoká, že výsledná hodnota NPV dosáhne milionových hodnot. Je ovšem pravděpodobnější, že bude dosahováno ztráty, která je v průměru v několika desítkách tisíc korun.

Tabulka 4-4: Vybrané hodnoty NPV- 1. varianta

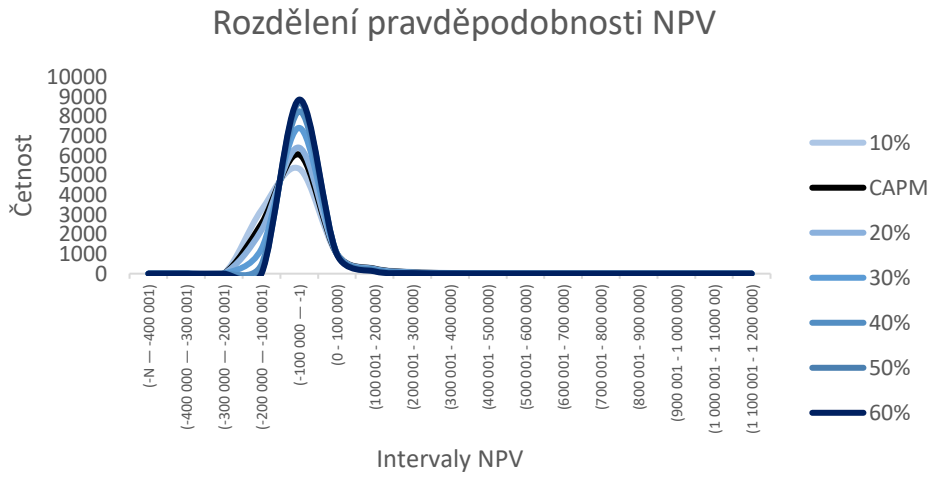
	NPV (CZK)				
Míra výnosnosti	Maximum	Minimum	Medián	Průměr	Sm. odchylka
10 %	3 036 638	-293 401	-81 270	-14 136	249 463
CAPM	2 788 460	-270 732	-79 271	-19 251	222 993
20 %	2 679 729	-261 064	-78 464	-21 535	211 710
30 %	2 394 097	-237 020	-76 479	-27 665	183 025
40 %	2 160 719	-218 622	-75 266	-32 817	160 660
50 %	1 966 691	-203 898	-74 706	-37 201	142 836
60 %	1 802 980	-191 905	-74 201	-40 972	128 362

Zdroj: vlastní zpracování

Hned na počátku investování finančních prostředků k nákupu těžících zařízení čelí potenciální investor rozhodnutí o počtu zařízení, které za účelem těžby nakoupí. Množství je závislé na disponibilních zdrojích subjektu, nicméně je důležité zdůvodnit své rozhodnutí a podepřít ho fakty. V návaznosti na tento problém v rozhodování je provedeno porovnání ziskovosti těžby v případech nákupu jednoho a dvou přístrojů určených k těžbě. Výsledky druhé možnosti jsou shrnuty výše v rámci popisu první varianty. Výsledky první možnosti, tedy nákup pouze jednoho těžícího zařízení, jsou součástí následujícího textu.

Těžbou s využitím jediného přístroje je možné docílit nižších ztrát, ale také nižších zisků, což je patrné z grafu 4-7. Pro většinu scénářů vychází čistá současná hodnota v rozmezí od -200 000 CZK do 100 000 CZK, přičemž nižší hodnota NPV než -200 000 CZK, nevychází u žádného ze scénářů. Nižší hodnoty ztrát, jak již bylo zmíněno, jsou ovšem kompenzovány poklesem očekávaného zvýšení hodnoty majetku u scénářů s kladnou NPV. Je tomu tak, protože náklady jsou fixní a výraznější nárůst ceny bitcoinu způsobí vyšší kladný efekt u varianty s využitím dvou těžících zařízení, neboť je vytěženo dvojnásobné množství bitcoinů. Naopak v případě výrazného poklesu ceny je výhodnější těžba s využitím jednoho přístroje, neboť jsou minimalizovány ztráty způsobené fixními náklady.

Graf 4-7: Rozdělení pravděpodobnosti NPV - 1. varianta (1 těžící zařízení)



Zdroj: vlastní zpracování

Jak vyplývá z tabulky 4-5, maximální výše NPV se oproti možnosti těžby s dvěma přístroji výrazně snížila. Těžař nemá možnost využít potenciálu zvýšené ceny, pokud vytěží menší množství bitconů. Oproti tomu je limitován nižší maximální ztrátou z projektu, protože fixní náklady na elektřinu jsou poloviční. Medián je mírně nižší, než v případě využití dvou těžících zařízení, nicméně průměrná hodnota NPV se značně snížila, neboť u scénářů s kladnou NPV nedosahují tyto NPV tak vysokých hodnot, jako v případě těžby s dvěma přístroji na těžbu. Směrodatná odchylka je také nižší, což odpovídá zúženému rozdělení pravděpodobnosti, jež je patrné z grafu 4-7.

Tabulka 4-5: Vybrané hodnoty NPV - 1. varianta (1 těžící zařízení)

	NPV (CZK)				
Míra výnosnosti	Maximum	Minimum	Medián	Průměr	Sm. odchylka
10 %	1 158 116	-160 720	-79 894	-59 867	80 712
CAPM	1 074 663	-146 347	-74 391	-56 204	73 017
20 %	1 037 829	-140 276	-72 084	-54 679	69 749
30 %	940 145	-125 016	-66 316	-50 926	61 460
40 %	859 176	-113 329	-61 808	-48 159	54 994
50 %	790 915	-104 401	-58 589	-46 087	49 818
60 %	732 548	-98 106	-55 960	-44 515	45 582

Zdroj: vlastní zpracování

V porovnání s možností těžby s využitím dvou přístrojů je počet scénářů se zápornou hodnotou výrazně vyšší, viz. tabulka 4-6. Ukazuje se tak, že s předpokládaným růstem ceny bitcoinu je výhodnější investovat do více těžících zařízení, neboť výnos je variabilní a přímo úměrný počtu vytěžených bitcoinů, kdežto náklady jsou fixní.

Tabulka 4-6: Poměr kladných a záporných NPV - 1. varianta (1 těžící zařízení)

Míra výnosnosti	10 %	CAPM	20 %	30 %	40 %	50 %	60 %
NPV < 0	8 586	8 615	8 634	8 691	8 735	8 798	8 862
NPV > 0	1 414	1 385	1 366	1 309	1 265	1 202	1 138

Zdroj: vlastní zpracování

4.2.2 **Optimistická varinta**

Optimistická varianta je založena na predikci ceny bitcoinového obchodníka, který si říká Masterluc. Důvodem výběru této předpovědi, která bude určovat poteniální ziskovost projektu, je kvalita minulých předpovědí daného obchodníka. V roce 2017 předpověděl nárůst ceny bitcoinu ke konci daného roku na hodnotu 15 000 dolarů[19], což se ukázalo jako správná predikce. Jeho nejnovější predikce je výrazně optimistická a předpokládá nárůst ceny na hodnotu mezi 40 000 – 110 000 dolarů[20]. Jelikož už právě varianta nárůstu ceny bitcoinu v roce 2019 na 40 000 USD je vysoce optimistická, bude v rámci simulace počítáno s touto hodnotou, jako očekávanou střední hodnotou všech scénářů po prvním roce.

Relevantní měsíční data pro tuto variantu pocházejí z počátku druhého měsíce roku 2017 až do 1. 2. 2018, nikoliv z posledních tří let jako u prvního a třetího scénáře. Důvodem je

[19] Odkaz: http://www.bitcoincasinos.com/blog/bitcoin-trader-predicts-digital-currency-will-scale-to-15000-in-2017/
[20] Odkaz: https://cointelegraph.com/news/legendary-bitcoin-trader-masterluc-predicts-15000-bitcoin-this-year

vybraná predikce obchodníkem, který si říká Masterluc, neboť svou předpověď formuloval s přihlédnutím k vývoji v roce 2017, což byl rok, kdy bitcoin vzrostl až na vysokých 18 700 USD. Data jsou proto vybrána tak, aby směrodatná odchylka odpovídala vývoji ceny v posledním roce a byla tak zaručena konzistence s predikcí. Simulace ceny je provedena na základě těchto dat, přičemž střední hodnota je zvolena tak, aby průměrná cena v roce 2019 přesáhla 40 000 USD (806 520 CZK):

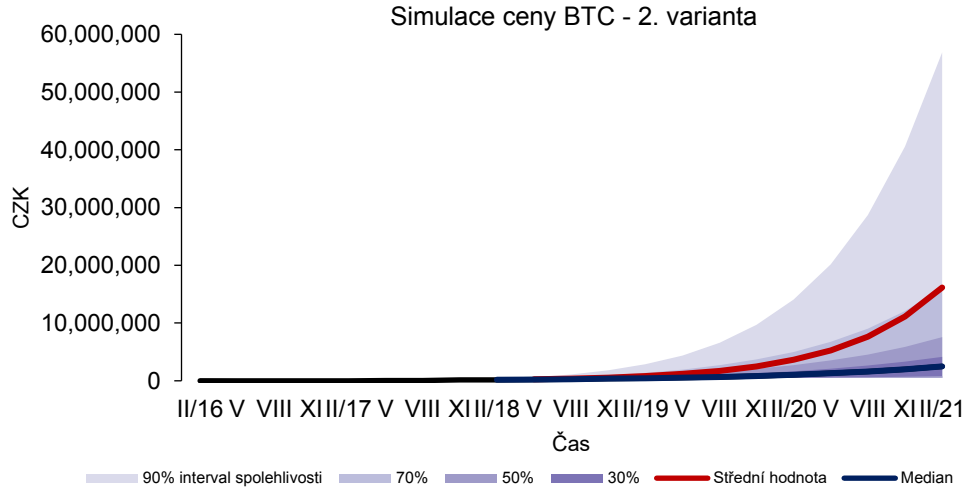
Tabulka 4-7: Vstupní údaje pro 2. variantu

	Hash rate	Cena
Střední hodnota	58.22 %	149 %
Směrod. Odchylka	30.46 %	120.02 %
Interval	0.083333	0.083333
Výchozí hodnota	2.07E+10 GH/s	184 905 CZK

Zdroj: vlastní zpracování

Jak je zřejmé z grafu 4-8, rozdělení výsledných simulovaných cen je kladně zešikmeno. Výrazný nárůst střední hodnoty během tří let projektu ze 184 905 CZK na 16 152 747 CZK je způsoben hlavně extrémně velkým vzrůstem ceny u přibližně 20 % scénářů, u kterých je konečná simulovaná cena vyšší, než střední hodnota.

Graf 4-8: Simulace ceny bitcoinu - 2. varianta

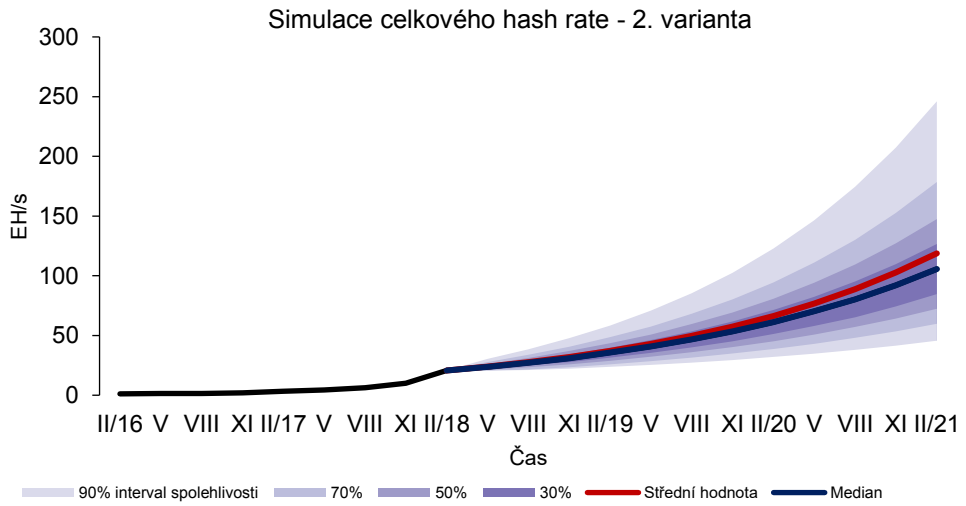


Zdroj: vlastní zpracování

V rámci 90 % intervalu spolehlivosti může cena u některých scénářů vzrůst až k 56 866 359 CZK nebo se snížit na 60 934 CZK. Medián k datu 2. 2. 2021 je 2 491 270 CZK, z čehož vyplývá, že konečná cena bitcoinu je pro 50 % scénářů značně nižší, než střední hodnota.

Průměrný hash rate celé sítě má rostoucí tendenci po celé tříleté období, viz. graf 4-9, a přírůstek výchozí hodnoty 20.7 EH/s činí za první rok 16.4 EH/s. Za celé období je to 98.1 EH/s a průměrná hodnota je 118.8 EH/s. Razantní nárůst výpočetní síly odpovídá velkému nárůstu ceny bitcoinu, neboť značně rostoucí cena ovlivní rozhodování mnoha lidí a poskytne jim incentivu k těžbě. Medián hash rate ke konci projektu činí 105.7 EH/s, přičemž vývoj mediánu je velmi podobný vývoji střední hodnoty. To znamená, že hash rate extrémně nenarůstá pouze u malého procenta scénářů, ale vysoký nárůst je signifikantní pro velkou část celkových scénářů. Konečné rozmezí hash rate k 2. 2. 2021 v rámci 90% intervalu spolehlivosti je 43 EH/s – 246 EH/s. U 90 % scénářů je tak hash rate minimálně dvojnásobný oproti výchozí hodnotě. V souvislosti s vysokým nárůstem ceny je takový vývoj hash rate zcela v souladu s myšlenkou, že stále výraznější nárůst ceny je doprovázen nárůstem výpočetního výkonu.

Graf 4-9: Simulace hash rate - 2. varianta

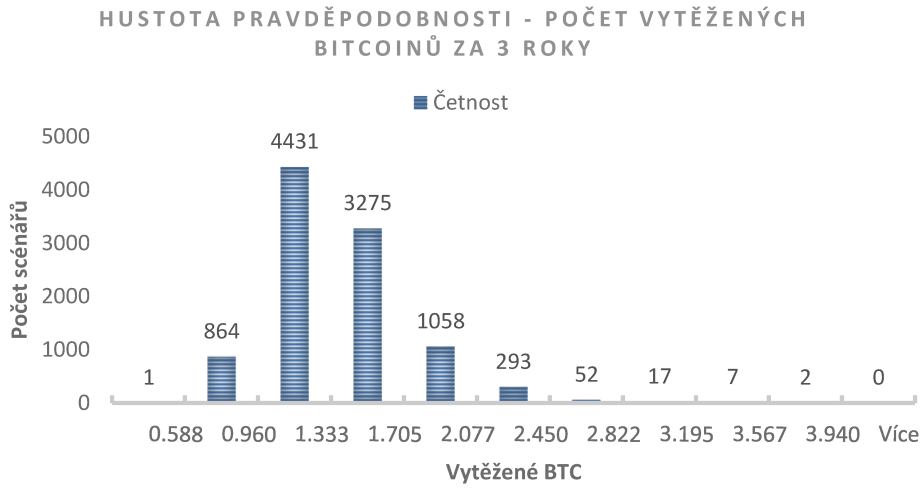


Zdroj: vlastní zpracování

Čistá současná hodnota – 2. varianta

Vzhledem k nastaveným parametrům simulace a odlišnému vývoji hashrate, je konečný počet vytěžených bitcoinů u většiny scénářů nižší, než v předchozí variantě, viz graf 4-10. Pro největší počet scénářů vychází množství vytěžených bitcoinů v rozmezí 0.96 – 1.33. Maximální počet vytěžených bitcoinů činí 3.94. Naopak minimální hodnota činí 0.588 vytěžených bitcoinů. Rozdělení vytěžených bitcoinů je, obdobně jako rozdělení simulovaných hodnot hash rate, kladně zešikmeno, což je logické, neboť počet vytěžených bitcoinů se odvíjí od celkového výpočetního výkonu bitcoinové sítě.

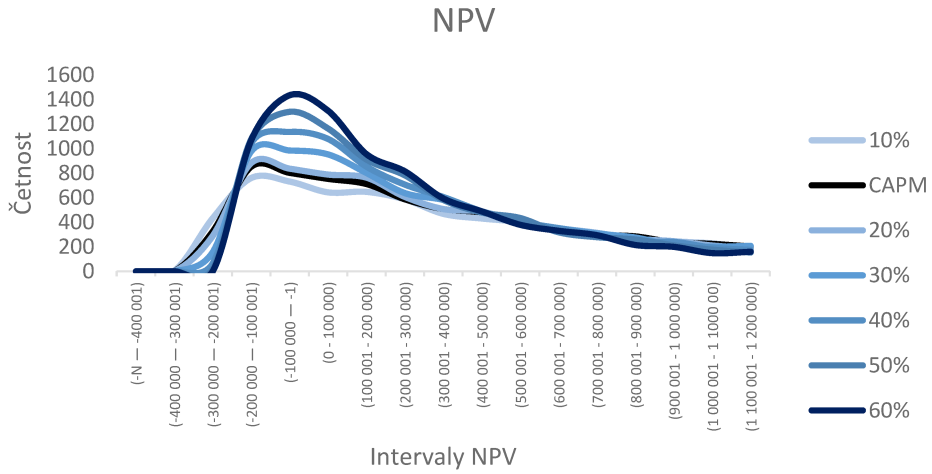
Graf 4-10: Celkový počet vytěžených bitcoinů – 2. varianta



Zdroj: vlastní zpracování

Graf 4-11 hustoty pravděpodobnosti čisté současné hodnoty je výrazně odlišný od grafu 4-5. Množství scénářů v rámci jednotlivých intervalů je nižší a signifikuje větší rovnoměrnost rozložení a větší počet scénářů v intervalech s kladnou NPV, zejména pak v intervalech od 100 000 CZK. S roustoucí požadovanou mírou výnosnosti se zvyšuje počet scénářů s NPV v rozmezí od -200 000 do 400 000 CZK, přičemž nejvyšší nárůst počtu scénářů z 721 na 1 438 je zaznamenán v prvním záporném intervalu, neboť se zvyšující se diskontní sazbou klesá současná hodnota budoucích ztrát.

Graf 4-11: Rozdělení pravděpodobnosti NPV - 2. varianta



Zdroj: vlastní zpracování

Celkové rozdělení scénářů z hlediska kladné a záporné čisté současné hodnoty odpovídá značně optimistickým předpokladům stanovených v této variantě. Dle tabulky 4-8 je pro každou míru požadované výnosnosti pravděpodobnost dosažení kladné NPV vyšší než 74 %.

Tabulka 4-8: Poměr kladných a záporných NPV – 2. varianta

Míra výnosnosti	10 %	CAPM	20 %	30 %	40 %	50 %	60 %
NPV < 0	1 929	1 980	2 007	2 118	2 243	2 393	2 503
NPV > 0	8 071	8 020	7 993	7 882	7 757	7 607	7 497

Zdroj: vlastní zpracování

V tabulce 4-9 jsou shrnuty důležité hodnoty NPV pro vybrané míry výnosnosti. Maximální hodnota NPV všech 10 000 scénářů je rovna 139 257 914 CZK při nejnižší uvažované diskontní míře 10 %. S rostoucí mírou výnosnosti maximální hodnota NPV klesá, oproti tomu minimum je se zvyšující se diskontní mírou rostoucí. Pro medián, průměr a směrodatnou odchylku platí obdobný závěr jako v případě maxima, neboť klesá současná hodnota budoucích peněžních toků.

Tabulka 4-9: Důležité hodnoty NPV - 2. varianta

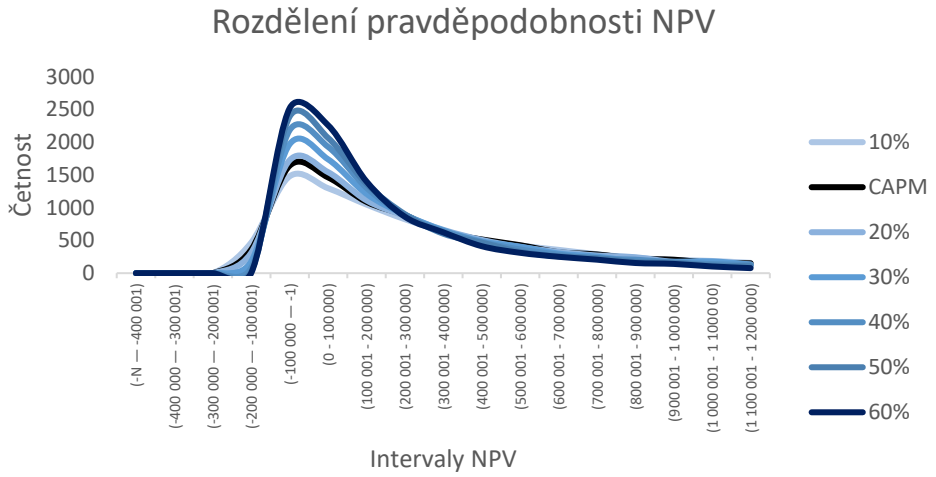
	NPV(CZK)				
Míra výnosnosti	Maximum	Minimum	Medián	Průměr	Sm. odchylka
10 %	139 257 914	-328 515	570 534	1 728 004	4 401 608
CAPM	117 041 893	-300 210	496 050	1 493 487	3 772 641
20 %	107 839 459	-288 228	463 881	1 394 672	3 510 220
30 %	85 274 917	-258 028	383 288	1 147 127	2 860 784
40 %	68 643 939	-234 794	319 585	958 520	2 375 035
50 %	56 111 403	-216 518	268 264	811 638	2 003 444
60 %	46 484 255	-201 867	227 660	695 071	1 713 575

Zdroj: vlastní zpracování

Při využití jednoho těžícího zařízení je počet scénářů v jednotlivých intervalech méně rovnoměrně rozložen, jak je zřejmé z grafu 4-12. Snížením počtu těžících zařízení na jeden kus je snížena možnost maximální ztráty, protože posledním záporným intervalem, do něhož spadají některé ze scénářu, je interval od -200 000 do -100 000 CZK. Je též zřejmé, že dojde ke snížení počtu scénářů s výrazně vysokou NPV, protože nebude využit potenciál velmi vysoké ceny bitcoinu v souvislosti s množství vytěžených bitcoinů. Jak bylo již zmíněno u předchozí varianty, s fixními náklady na jedno zařízení a rostoucí cenou bitcoinů, je větší počet těžících

zařízení faktorem zvyšující efektivnost z celkové investice. Pokud je tedy předpokládán výrazný nárůst ceny, je vhodné nakoupit větší množství zařízení určených k těžbě.

Graf 4-12:Rozdělení pravděpodobnost NPV - 2. vairanta (1 těžící zařízení)



Zdroj: vlastní zpracování

Jak již bylo zmíněno v předchozím odstavci, snížením počtu těžicích zařízení nebude plně využit potenciál výrazného nárůstu ceny, což se projeví jednak v případě maximální NPV, jež je značně nižší, ale jednak se sníží výsledná NPV u velkého počtu scénářů, jak signifikuje medián, který je přibližně poloviční oproti možnosti s dvěma zařízeními, viz tabulka 4-10.

Tabulka 4-10: Vybrané hodnoty NPV - 2. varianta (1 těžící zařízení)

	NPV (CZK)				
Míra výnosnosti	Maximum	Minimum	Medián	Průměr	Sm. odchylka
10 %	69 627 447	-167 107	283 757	862 373	2 200 849
CAPM	58 519 598	-152 590	246 675	745 293	1 886 360
20 %	53 918 451	-146 445	230 661	695 961	1 755 147
30 %	42 636 356	-130 962	190 541	572 382	1 430 423
40 %	34 321 005	-119 053	158 821	478 228	1 187 545
50 %	28 054 847	-109 688	133 208	404 908	1 001 745
60 %	23 241 362	-102 182	113 000	346 721	856 808

Zdroj: vlastní zpracování

Odstraněním jednoho těžícího zařízení se z hlediska poměru mezi scénáři s výslednou kladnou a zápornou NPV mnoho nezmění, jak dokládá tabulka 4-11. Změna oproti možnosti s dvěma přistroji na těžbu je minimální, neboť u značné části scénářů dosahuje NPV tak vysokých hodnot, že rozdílné množství těžících přístrojů nezpůsobí pokles NPV do záporných hodnot. Důvodem je také relativně vysoká cena bitcoinu na konci jednotlivých roků, která

zachová těžbu ziskovou i v případě poloviční výpočetního výkonu přístrojů těžaře o polovinu.

Tabulka 4-11: Poměr kladných a záporných NPV - 2. varianta (2 těžící zařízení)

Míra výnosnosti	10 %	CAPM	20 %	30 %	40 %	50 %	60 %
NPV < 0	1 945	2 000	2 034	2 148	2 263	2 414	2 518
NPV > 0	8 055	8 000	7 966	7 852	7 737	7 586	7 482

Zdroj: vlastní zpracování

4.2.3 **Pesimistická varianta**

Protože je důležité počítat také s propadem hodnoty bicoinu, bude poslední scénář výrazně pesimistický. Ačkoli mnoho lidí předpovídá pád bitcoinu, daná simulace nebude založena na žádné konkrétní předpovědi. Výchozí data budou zvolena zcela intuitivně tak, aby docházelo k postupnému snižování hodnoty, nikoli aby došlo k prudkému propadu. Vyjma střední hodnoty pro výpočet simulace ve velikosti -30 % u ceny a -15 % u hash rate, jsou ostatní hodnoty stejné jako v případě scénáře prvního.

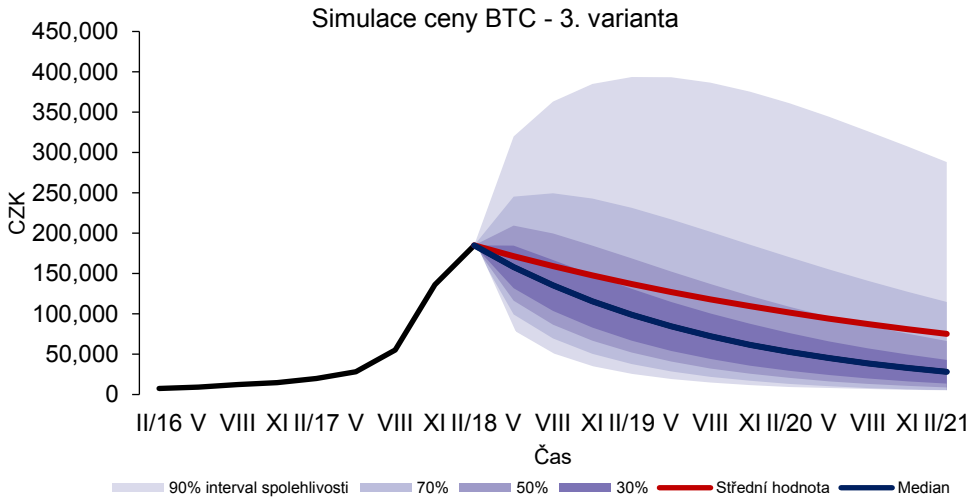
Tabulka 4-12: Vstupní údaje – 3. varianta

	Hash rate	Cena
Střední hodnota	-15.00 %	-30.00 %
Směrod. Odchylka	32.84 %	87,36 %
Interval	0.083333	0.083333
Výchozí cena BTC	2.07E+10 GH/s	184 905 CZK

Zdroj: vlastní zpracování

Jak je zřejmé z grafu 4-13, střední hodnota ceny v rámci pesimistického scénáře postupně klesá z 184 905 CZK až k 75 177 CZK v roce 2021. Pokles střední hodnoty není faktorem zaručujícím ztrátu v projektu, neboť pokles ceny může být do určité míry kompenzován zvyšujícím se množstvím vytěžených bitcoinů, v případě poklesu celkové výpočetní síly bitcoinové sítě. Snižující se hodnota je patrná také u mediánu, tento pokles je ale výraznější, než u střední hodnoty. Pokles střední hodnoty je nižší, neboť simulované ceny jsou kladně zešikmeny. Z konečné hodnoty mediánu ve výši 28 122 CZK vyplývá, že u poloviny scénářů dochází v průběhu tří let k poklesu ceny minimálně o 156 783 CZK. Rozpětí cen je u 90 % scénářů nižší, než v případě předchozích dvou variant a činí 286 296 CZK, přičemž hranice intervalu jsou 1 986 CZK – 288 282 CZK.

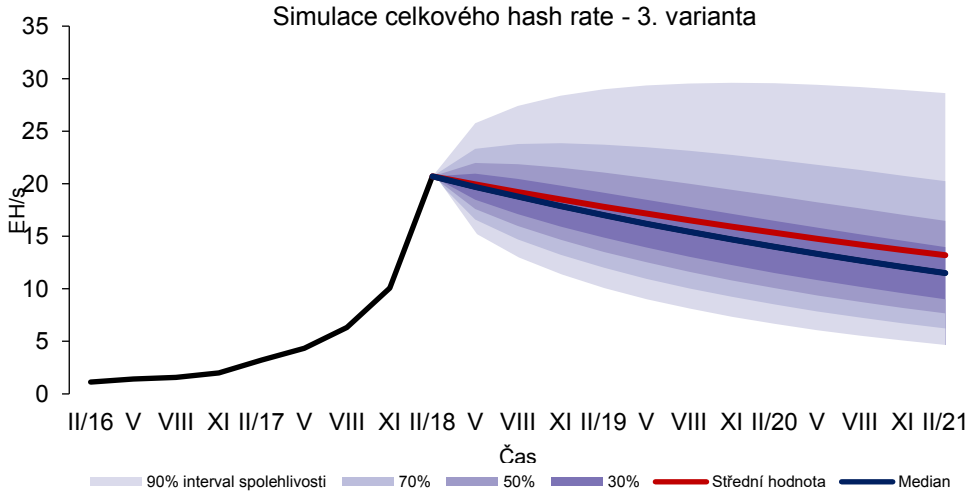
Graf 4-13: Simulace ceny bitcoinu - 3. varianta



Zdroj: vlastní zpracování

Jak již bylo zmíněno v popisu základních charakteristik scénářů, postupný pokles ceny v případě pesimistické varianty je doprovázen poklesem celkového výpočetního výkonu, viz graf 4-14. To lze demonstrovat na vývoji mediánu a střední hodnoty celkového hash rate, která ve výchozím měsíci činila 20.7 EH/s a postupným poklesem po dobu tří let se snížila na hodnotu 13.2 EH/s. Přesto se stále jedná o obrovský výpočetní výkon bitcoinové sítě, pokud je brána v potaz spotřeba elektřiny. Medián je na konci období projektu mírně nižší a činí 11.5 EH/s. Konečný hash rate pro 9 z 10 scénářů vychází v intervalu od 4.40 EH/s do 28.62 EH/s. Pro polovinu scénářů je to interval od 7.65 EH/s do 16.48 EH/s.

Graf 4-14: Simulace hash rate - 3. varianta

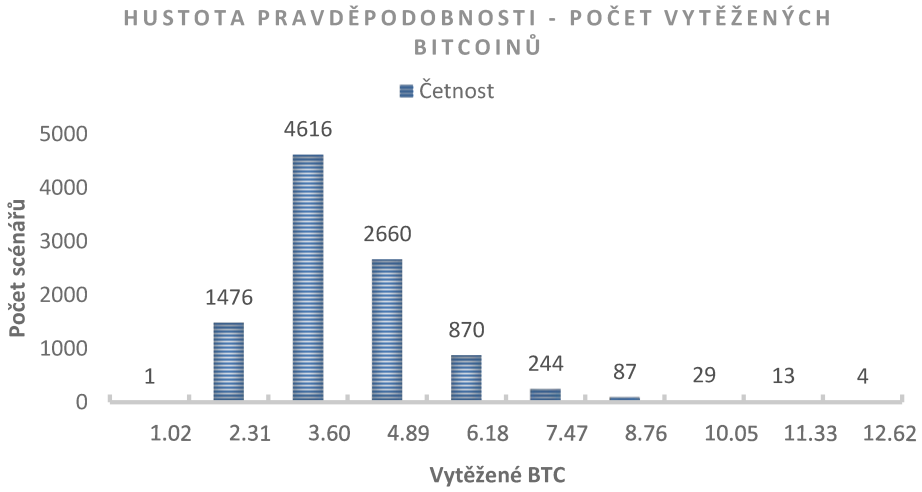


Zdroj: vlastní zpracování

Čistá současná hodnota – 3. varianta

Klesající hashrate má vliv na množství vytěžených bitcoinů jednotlivcem při zachování výpočetního výkonu s kterým bitcoiny těží. Protože se zvyšuje jeho procentní zastoupení na celkovém výpočetním výkonu, roste i předpokládaná odměna. Tato skutečnost je dobře viditelná z grafu 4-15, který je zaměřen na počet vytěžených bitcoinů při pesimistickém vývoji předpokládáném v této konkrétní variantě. Oproti předchozím variantám jsou intervaly vytěžených bitcoinů za tři roky investice, do kterých spadají jednotlivé scénáře, výrazně vyšší. U největšího počtu scénářů je rozmezí předpokládaného množství od 2,31 BTC – 3,60 BTC. Pravděpodobnější zisk odměny je ovšem kompnezován razantním poklesem hodnoty bitcoinu, proto nelze jednoznačně mluvit o pozitivním jevu.

Graf 4-15: Celkový počet větěžených bitcoinů - 3. varianta



Zdroj: vlastní zpracování

Jak bylo zmíněno, počet vytěžených bitcoinů sám o sobě neznamená jistotu dosahování zisku z investice. Potvrzením této myšlenky je tabulka 4-13, z které je patrné, že u naprosté většiny scénářů vychází NPV záporná a projekt je nevhodný k realizování. Vysoký pokles hodnoty bitcoinu již několikrát nastal, proto je důležité brát na vědomí i tuto možnost. Ačkoli je těžař limitován maximální možnou ztrátou zahrnující počáteční a průběžné výdaje, v předchozích variantách má relativně velkou pravděpodobnost dosažení velmi vysokých hodnot NPV. V pesimistické variantě je tato pravděpodobnost velmi nizká a z celkového počtu scénářů, kdy je NPV kladná, je většina v intervalu od 0 – 100 000 CZK, viz. graf 4-16.

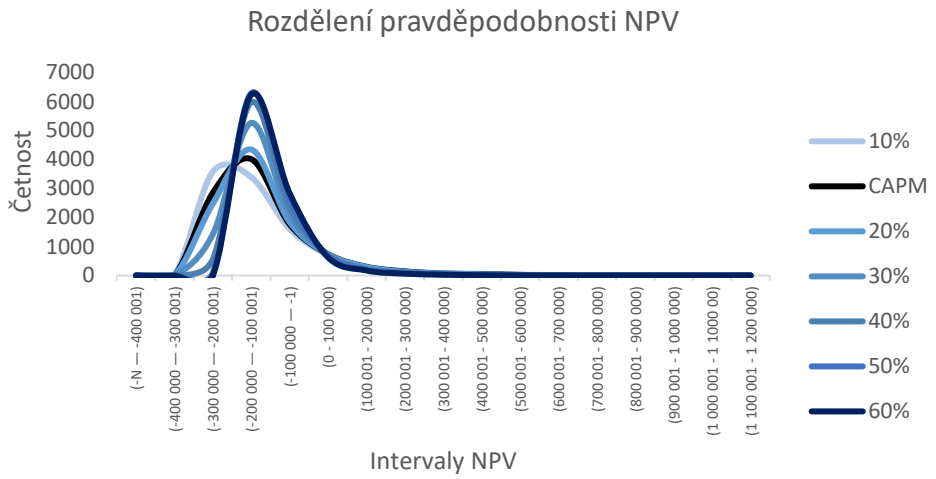
Tabulka 4-13:Poměr kladných a záporných NPV - 3. varianta

Míra výnosnosti	10 %	CAPM	20 %	30 %	40 %	50 %	60 %
NPV < 0	8 591	8 642	8 674	8 778	8 883	8 979	9 079
NPV > 0	1 409	1 358	1 326	1 222	1 117	1 021	921

Zdroj: vlastní zpracování

Dle dat v tabulce 4-13 je scénářů se zápornou hodnotou NPV v každé variantě požadované míry výnosnosti více než 85 %. Z těchto 85 % je nejvíc v intervalu NPV od -200 000 CZK do -100 000 CZK, jak je patrné z grafu 4-16, a tento počet postupně narůstá se zvýšenou diskonstní sazbou z 3 399 až na 6 239 scénářů. Nárůst je způsoben zejména poklesem množství scénářů, s konečnou NPV nižší než -200 000 CZK z 3 579 scénářů na 0, se zvyšující se mírou výnosnosti.

Graf 4-16: Rozdělení pravděpodobnosti NPV - 3. varianta



Zdroj: vlastní zpracování

Z hlediska maximální hodnoty a směrodatné odchylky NPV je patrný klesající trend se zvyšující se mírou výnosnosti, a naopak NPV minimální a průměrná spolu s mediánem roste, jak lze postřehnout z tabulky 4-14. Užitím kritéria průměrné NPV je tak demonstrován vhodný argument pro nerealizaci projektu, neboť záporná průměrná data signifikují pravděpodobnou ztrátu z investice.

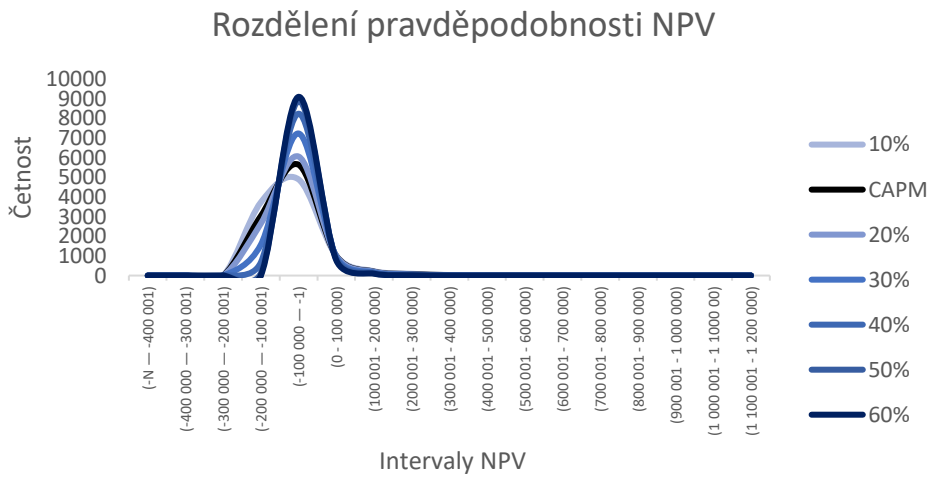
Tabulka 4-14: Vybrané hodnoty NPV - 3. varianta

	NPV (CZK)				
Míra výnosnosti	Maximum	Minimum	Medián	Průměr	Sm. odchylka
10 %	3 511 810	-313 125	-166 189	-124 466	159 257
CAPM	3 119 912	-286 251	-155 401	-118 182	142 848
20 %	2 952 489	-274 882	-150 941	-115 577	135 838
30 %	2 525 881	-246 252	-139 724	-109 190	117 964
40 %	2 192 445	-225 203	-131 164	-104 488	103 970
50 %	1 926 368	-209 485	-124 764	-100 955	92 772
60 %	1 710 228	-196 714	-119 568	-98 254	83 642

Zdroj: vlastní zpracování

Těžbou s jedním těžícím zařízením je možné zúžit celkový interval možných hodnot NPV, viz graf 4-17. Rozdělení v tomto případě je záporně zešikmeno a zvýšila se jeho špičatost. Protože dle varianty s využitím dvou zařízení je velká pravděpodosnost ztráty z projektu, využití pouze jednoho přístroje výrazně sníží fixní náklady, které nebudou pokryty výnosem z prodeje bitcoinů, čímž se sníží maximální možné ztráty u jednotlivých scénářů.

Graf 4-17: Rozdělení pravděpodobnosti NPV - 3. varianta (1 těžící zařízení)



Zdroj: vlastní zpracování

Průměr NPV je stále záporná hodnota, nicméně se jedná o hodnotu absolutně nižší, čímž se potvrzuje myšlenka, že s očekávaným poklesem ceny bitcoinu a hash rate dle předpokladů této varianty je výhodnější těžit pouze s jedním zařízením. Data z tabulky 4-15 rovněž odpovídají rozdělení pravděpodobnosti NPV zachyceném v grafu 4-17. Snížila se maximální hodnota NPV pro všechny míry požadované výnosnosti, ale také platí, že nejnižší hodnota, směrodatná odchylka a medián NPV jsou téměř poloviční.

Table 4-15: Vybrané hodnoty NPV - 3. varianta (1 těžící zařízení)

	NPV (CZK)				
Míra výnosnosti	Maximum	Minimum	Medián	Průměr	Sm. odchylka
10 %	1 754 395	-159 413	-84 855	-63 961	79 688
CAPM	1 558 608	-145 610	-79 275	-60 632	71 479
20 %	1 474 965	-139 772	-76 929	-59 250	67 971
30 %	1 261 838	-125 074	-71 145	-55 853	59 029
40 %	1 095 258	-113 785	-66 703	-53 344	52 027
50 %	962 329	-105748	-63 356	-51 450	46 424
60 %	854 349	-99 257	-60 684	-49 997	41 856

Zdroj: vlastní zpracování

Jak je patrné z tabulky 4-16, poměr záporných a kladných NPV se výrazněji nezměnil,což znamená, že změnou množství těžících přístrojů ze dvou na jediný se sníží hlavně velikost možné ztráty pro scénáře se zápornou NPV.

Tabulka 4-16: Poměr kladných a záporných NPV - 3. varianta (1 těžící zařízení)

Míra výnosnosti	10 %	CAPM	20 %	30 %	40 %	50 %	60 %
NPV < 0	8 626	8 679	8 708	8 806	8 912	9 008	9 100
NPV > 0	1 374	1 321	1 292	1 194	1 088	992	900

Zdroj: vlastní zpracování

4.3 Zhodnocení

Ziskovost těžby bitcoinů je závislá na velkém množství faktorů, které ovlivňují jednak náklady na těžbu, a jednak realizované výnosy. Náklady je možné optimalizovat výběrem nejlevnějšího dodavatele elektřiny, zvýhodněnou smlouvou ohledně platby za 1 MWh elektřiny nebo změnou země, kde bude těžba probíhat. Také jednorázové kapitálové výdaje je možné snížit výběrem levnějších těžících zařízení za cenu sníženého výkonu či efektivity. V některých případech je možné koupit konkrétní těžící zařízení za zvýhodněných nabídek nebo na bazarových stráknách, kde ovšem nemusí být zaručena odpovídající kvalita a výkon. Výnosy jsou na druhou stranu závislé na faktorech, jež ovlivnit nelze (pokud není brán v potaz možnost koupě většího množství zařízení), neboť cena je tvořena nabídkou a poptávkou a celkový výpočetní výkon sítě je od ceny do určité míry odvozen. V práci jsou stanoveny jasné předpoklady a vstupní data, nicméně na základě předchozí úvahy je jasné, že se předpoklady a data ohledně nákladů mohou různě lišit.

V případě vývoje ceny a hashrate odpovídající první variantě a se zvolenými předpoklady by nebylo vhodné investovat do těžících zařízení a těžit bitcoin. Důvodem je větší pravděpodobnost ztráty z dané investice, nicméně faktorů ovlivňujících tento výsledek je několik. Z hlediska nákladů je výsledek velmi ovlivněn náklady na těžící zařízení a náklady na elektřinu, které jsou relativně vysoké a v mnoha případěch převýší dosažený výnos z prodeje vytěžených bitcoinů. Těžař musí v případě zisku zaplatit 15% daň a 2% poplatek poolu, což také ovlivní končenou ziskovost. V souvislosti s výnosy je důvodem kombinovaný vývoj ceny a výpočetního výkonu. Nejlepší možnou kombinací je růst ceny a pokles výpočetního výkonu bitcoinové sítě nebo procentně vyšší nárůst ceny oproti procentnímu nárůstu výpočetního výkonu. Na základě získaných výsledků je pravděpodobnější, že zmíněné kombinace nedominují většině scénářů a změny ve vývoji ceny a hashrate nejsou kombinovaně natolik vhodné, aby těžba byla ve většině případů zisková.

Jestliže by se v reálném světě cena bitcoinu a výpočetní výkon vyvíjel tak, jak je předpokládáno v optimistické variantě, bylo by logické těžit a investovat do většího množství těžících přístrojů a zvážit možné varianty množství těchto zařízení. Pravděpodobnost, že bude dosaženo kladné NPV je pro všechny hodnoty diskontní sazby od 10 % do 60 % vyšší než 74 %. V některých případech, při pořízení dvou přístrojů k těžbě, je možné dosáhnout čisté současné hodnoty v řádech desítek milionů korun českých. Jedná se nicméně o výrazně optimistickou variantu a jednu z mnoha predikcí významných obchodníků či lidí zajímajících se o bitcoin. Je proto potřebné si před samotnou těžbou umět zdůvodnit proč by se bitcoin měl vyvíjet takhle. V práci je tato varianta brána jako jedna z možných a cílem je posoudit ziskovost v případě stanoveného vývoje. Proto je potřeba, než těžař začne investovat do těžících zařízení a těžit, zvážit pravděpodobnost, že tato varianta nastane.

Dle provedené analýzy pesimistické varianty je jasné, že v případě vývoje hashrate a ceny na základě zvolených předpokladů je těžba z naprosté většiny případů ztrátová. Vzhledem k tomu, že je predikován výrazný pokles ceny, není vhodné investovat do těžících zařízení pokud těžař nedosahuje opravdu nízkých nákladů na elektřinu, neboť právě ty tvoří největší část nákladů. Jestliže existují těžaři, kteří mají konkurenční výhodu z hlediska nákladů na elektřinu, budou tito vytlačovat z trhu těžaře s vyššími náklady. Jedná se o logickou konkluzi, neboť pro zvýhodněné těžaře bude těžba při klesající ceně déle profitabilní. A tedy první, kdo těžby zanechá, bude těžař dosahující ztrát dříve, čímž též minimalizuje očekávanou výši těchto ztrát. Navíc těžaři dosahující nižších nákladů budou na tuto chvíli čekat, neboť poté se začne snižovat výpočetní výkon a budou tak inkasovat větší odměny.

5 Závěr

Bitcoin se stal v roce 2017 fenoménem, který zaznamenal téměř každý člověk. Přestože je mnoho lidí, kteří principům bitcoinu a kryptoměn obecně nerozumí, najde se dost takových, kteří tématu rozumí natolik dobře, aby byli schopni s využitím svých znalostí z bitcoinu profitovat. Jednou z možností, jak na bitcoinu zbohatnout je bitcoin začít těžit. S využitím svých technických dovedností a finančních prostředků se o to mnoho lidí pokusilo. Kolik uspělo a kolik ne, a je-li těžba dnes výnosná, je otázkou.

Cílem diplomové práce je posoudit ziskovost těžby bitcoinu za stanovených podmínek a potažmo seznámit čtenáře s tímto tématem.

Práce je spolu s úvodem a závěr rozdělena do pěti kapitol. Hned po úvodu následuje druhá kapitola. Obsahem druhé kapitoly je charakteristika bitcoinu se zaměřením na těžbu této kryptoměny. Nejprve je popsána historie bitcoinu od samotného vzniku až k razantnímu nárůstu jeho hodnoty ke konci roku 2017. Část následující je věnována ekonomickým myšlenkám, které korespondují s principy kryptoměn obecně. Po stručném popisu základních charakteristik bitcoinu je zbylá část kapitoly zaměřena na těžbu bitcoinu, kde jsou sepsány ‚spolu s principy těžby, různé možnosti těžby se zaměřením na těžbu v poolu.

Začátkem třetí kapitoly je popsáno finanční modelování, jako nástroj k zlepšení investičního rozhodování. Následuje popis simulace náhodného vývoje ceny finančního aktiva a simulace Monte Carlo. Další část je věnována investičnímu rozhodování se zaměřením na fáze investičního procesu, zdroje financování investic, parametry a kritéria hodnocení projektů jako čistá současná hodnota, vnitřní výnosové procento a doba úhrady. V rámci této kapitoly jsou popsány také náklady kapitálu, cizího i vlastního.

Ve čtvrté kapitole jsou nejprve definovány předpoklady a popsány vstupní data. Pokračování kapitoly je zaměřeno na výsledky simulace náhodného vývoje ceny bitcoinu a hash rate pro tři vybrané varianty, které se odlišovaly vstupními předpoklady. Následně je posouzena ziskovost těžby bitcoinu s využitím metody čisté současné hodnoty. Kapitola je zakončena zhodnocením výsledků.

Seznam literatury

Odborná kniha:

[1] DLUHOŠOVÁ, Dana. *Finanční řízení a rozhodování podniku.* 3. upr. vyd. Praha: Ekopress, 2010. 225 s. ISBN 978-80-86929-68-2.

[2] KRÁL, Bohumil a kol. *Manažérské účetnictví*. 3. dopl. a aktualiz. vyd. Praha: Management Press, 2010. ISBN 978-80-7261-217-8.

[3] POPPER, Nathaniel. *Digital gold: The untold story of bitcoin.* United States of America: HarperCollins Publishers, 2015. ISBN 978-0-241-18099-0.

[4] STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky.* 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1.

[5] ZMEŠKAL, Z., D. DLUHOŠOVÁ a T. TICHÝ. *Finanční modely: Koncepty, metody, aplikace*. 3., přep. a rozš. vyd. Praha: Ekopress, 2013. 267 s. ISBN 978-80-86929-91-0.

[6] ZMEŠKAL, Zdeněk, Miroslav ČULÍK a Tomáš TICHÝ. *Finanční rozhodování za rizika: sbírka řešených příkladů.* 4., upr. vyd. Ostrava: VŠB-TU Ostrava, 2013. ISBN 978-80-248-3249-4.

Internetové zdroje:

[7] 99BITCOINS. *Antminer S9 review.* [online]. 99.bitcoins [2. 1. 2018]. Dostupné z: https://99bitcoins.com/antminer-s9-review/

[8] BITCOINCASINOS.COM. *BITCOIN TRADER PREDICTS DIGITAL CURRENCY WILL SCALE TO $15,000 IN 2017.* [online]. Bitcoincasinos.com [18. 8. 2017]. Dostupné z: http://www.bitcoincasinos.com/blog/bitcoin-trader-predicts-digital-currency-will-scale-to-15000-in-2017/

[9] BLOCKCHAIN.INFO. *Bitcoin Block Explorer: Total Number of Transactions.* [online]. Blockhain.info [1. 2. 2018]. Dostupné z: https://blockchain.info/charts/n-transactions-total?timespan=all

[10] BLOCKCHAIN.INFO. *Bitcoin Block Explorer – Hash rate* [online]. Blockhain.info [1. 2. 2018]. Dostupné z: https://blockchain.info/charts/hash-rate

[11] BLOG.COINGATE. *How to setup Electrum and receive bitcoins.* [online]. [1. 2. 2017]. Dostupné z: https://blog.coingate.com/2017/02/setup-electrum-guide/

[12] BITCOINTALK. *Bitcoin forum – (Review/Guide) Antminer S9* [online]. Bitcointalk [2. 1. 2018]. Dostupné z: https://bitcointalk.org/index.php?topic=2676763.0

[13] BITCOINTALK. *How much times dows it takes to mine a block solo.* [online]. Bitcointalk [28. 9. 2015]. Dostupné z: https://bitcointalk.org/index.php?topic=1219836.0

[14] BITCOINWISDOM. *Bitcoin difficulty.* [online]. Bitcoinwisdom [2. 1. 2018]. Dostupné z: https://bitcoinwisdom.com/bitcoin/difficulty

[15] BUSINESS CENTER. *Zákon o daních z příjmů.* [online]. [1. 2. 2018]. Dostupné z: https://business.center.cz/business/pravo/zakony/dprij/prilos1.aspx

[16] BUY BITCOIN WORLDWIDE. *Halong Mining DragonMint 16T Review: Profitable or a Scam?* [online]. Buybitcoinworldwide [21. 3. 2018]. Dostupné z: https://www.buybitcoinworldwide.com/mining/hardware/dragonmint-16t/

[17] COINDESK. *Bitcoin hash functions explained*. [online]. Coindesk [19. 2. 2017]. Dostupné z: https://www.coindesk.com/bitcoin-hash-functions-explained/

[18] COINDESK. *Bitcoin (USD) price.* [online]. Coindesk [1. 2. 2017]. Dostupné z: https://www.coindesk.com/price/

[19] COINMAP.ORG *Map view – Czech Republic.* [online]. Coinmap [1. 2. 2018]. Dostupné z: http://www.coinmap.org

[20] COINTELEGRAPH. *Legendary Bitcoin Trader "masterluc" Predicts $15,000 Bitcoin This Year.* [online]. Cointelegraph [15. 8. 2017]. Dostupné z: https://cointelegraph.com/news/legendary-bitcoin-trader-masterluc-predicts-15000-bitcoin-this-year

[21] CZSO.CZ. *Spotřeba paliv a energií v domácnostech Středočeského kraje.* [online]. CZSO.cz [14. 3. 2017]. Dostupné z: https://www.czso.cz/csu/xs/spotreba-paliv-a-energii-v-domacnostech-stredoceskeho-kraje

[22] DAMODARAN ONLINE. *Home Page for Aswath Damodaran*. [online]. Damodaran online [1. 1. 2018]. Dostupné z: http://pages.stern.nyu.edu/~adamodar/

[23] DATABITCOINITY.ORG *Bitcoin network hashrate* [online]. Databitcoinity.org [1. 2. 2018]. Dostupné z: https://data.bitcoinity.org/bitcoin/hashrate/all?c=m&g=15&t=a

[24] ELEKTRINA.CZ. *Vše o elektřině* [online]. Elektrina.cz [5. 6 2017]. Dostupné z: https://www.elektrina.cz/ceny-elektriny-v-evrope-2016

[25] FRED.STLOUISFED. *Stock market indexes – S&P 500.* [online]. Fred.Stlouisfed [1. 2. 2018]. Dostupné z: https://fred.stlouisfed.org/series/SP500

[26] KURZY.CZ. *Detail online kurzu USD/CZK*. [online]. Kurzy.cz [2. 2. 2018]. Dostupné z: https://www.kurzy.cz/kurzy-men/aktualni/CZK-USD/

[27] MĚŠEC.CZ. *Jak se daní virtuální měny? Část zisku odvedete vždy, bitcoin je pro berňák věc.* [online]. Měšec.cz [11. 12 2017]. Dostupné z: https://www.mesec.cz/clanky/jak-se-dani-virtualni-meny-cast-zisku-odvedete-vzdy-bitcoin-je-pro-bernak-vec/

[28] MULTPL.COM. *10 Year Treasury Rate by Year.* [online]. Multpl.com [1. 1. 2018]. Dostupné z: http://www.multpl.com/10-year-treasury-rate/table/by-year

[29] PRESHING.COM. *What is a Bitcoin, Really ?* [online].Preshing.com [24. 1. 2014]. Dostupné z: http://preshing.com/20140127/what-is-a-bitcoin-really/

[30] RIGHTO. *Bitcoin mining the hard way: the algorithms, protocols and bytes.* [online]. Righto.com [23. 2. 2014]. Dostupné z: http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

[31] SKUPINA-CEZ. *Ceníky.* [online]. CEZ.cz [1. 1. 2018]. Dostupné z: https://www.cez.cz/cs/podpora/ceniky.html

[32] SLUSHPOOL: *Těžba pro začátečníky*. [online]. Slushpool [cit. 2018-02-01]. Dostupné z: https://slushpool.com/help/get-started/mining_beginners.

[33] SLUSHPOOL: *Odměňovací systém.* [online]. Slushpool [cit. 2018-02-01]. Dostupné z: https://slushpool.com/help/manual/rewards.

[34] TECHRADAR.PRO. *Best ASIC devices for Bitcoin mining in 2018*. [online]. Techradar.pro [1. 1. 2018]. Dostupné z: https://www.techradar.com/news/best-asic-devices-for-bitcoin-mining-in-2018

Seznam zkratek

CZK – koruna česká

NPV – čistá současná hodnota

BTC – bitcoin

GB – gigabyte

GH/s – gigahash za sekundu

HR – hash rate

MH/s – megahash za sekundu

S&P – Standard and Poor's

TH/s – terrahash za sekundu

USD – americký dolar

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 27. 4. 2018

.....

Michal Ondruš

seznam příloh